PRIVACY POLICY & TERMS OF SERVICE

Medismo LifeTech

(Product of Allied BizTech Solutions Pvt Ltd)

Effective Date: April 1, 2025
Last Updated: October 22, 2025
Version: 1.0

TABLE OF CONTENTS

PART A: PRIVACY POLICY

1. INTRODUCTION AND APPLICABILITY

1.1 About This Policy

This Privacy Policy ("**Policy**") governs the collection, processing, storage, use, disclosure, and protection of Personal Data (as defined herein) by **Medismo LifeTech(Allied BizTech Solutions Pvt Ltd)** ("**Medismo**," "**we**," "**us**," or "**our**"), a company incorporated under the Companies Act, 2013, having its registered office at 1ST FLOOR, NO.4, WELDER STREET ANNA SALAI , CHENNAI, Tamil Nadu.

1.2 Products Covered

This Policy applies to all users of the following Medismo products and services (collectively, the "**Services**"):

1. **CareConnect AI** - Patient Journey Intelligence Platform
2. **PatientVoice Pro** - Patient Trust Intelligence Platform
3. **FieldVoice** - Voice-Powered Pharma CRM & Territory Intelligence

1.3 User Categories

This Policy applies to the following categories of users ("**Users**" or "**you**"):

- **Healthcare Providers**: Hospitals, clinics, nursing homes, diagnostic centers, and individual healthcare practitioners
- **Pharmaceutical Companies**: Manufacturers, distributors, and marketing organizations
- **Medical Representatives**: Field force personnel employed by pharmaceutical companies
- **Healthcare Professionals**: Doctors, nurses, specialists, and allied health professionals
- **Administrative Personnel**: Hospital administrators, CRM managers, and system administrators
- **Patients**: Individuals whose data may be processed through our Services (with appropriate consent)

1.4 Consent and Acknowledgment

By accessing or using our Services, registering an account, or providing your Personal Data, you:

- Acknowledge that you have read, understood, and agree to be bound by this Policy
- Consent to the collection, processing, storage, use, and disclosure of your Personal Data as described herein
- Confirm that you have the authority to provide consent on behalf of your organization (if applicable)
- Understand your rights under the Digital Personal Data Protection Act, 2023 ("**DPDP Act**")

1.5 Regulatory Compliance

This Policy is designed to comply with:

- Digital Personal Data Protection Act, 2023 (India)
- Information Technology Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Clinical Establishments (Registration and Regulation) Act, 2010
- Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
- Drugs and Cosmetics Act, 1940
- Uniform Code of Pharmaceutical Marketing Practices (UCPMP)
- NABH Standards (where applicable)

2. DEFINITIONS

For the purposes of this Policy, the following terms shall have the meanings assigned below:

"Anonymized Data" means data that has been processed in such a manner that it can no longer be attributed to a specific Data Principal, either directly or indirectly, and is not Personal Data under the DPDP Act.

"Consent" means a free, specific, informed, and unambiguous indication of a Data Principal's agreement to the processing of their Personal Data, as defined under Section 6 of the DPDP Act.

"Data Fiduciary" means Medismo, as the entity that determines the purpose and means of processing Personal Data, as defined under Section 2(i) of the DPDP Act.

"Data Principal" means the individual to whom the Personal Data relates, as defined under Section 2(j) of the DPDP Act.

"Data Processor" means any entity that processes Personal Data on behalf of Medismo, as defined under Section 2(k) of the DPDP Act.

"Data Protection Officer" or "DPO" means the designated individual responsible for overseeing data protection strategy and ensuring compliance with the DPDP Act.

"Personal Data" means any data about an individual who is identifiable by or in relation to such data, as defined under Section 2(t) of the DPDP Act, including but not limited to:

- Name, age, gender, date of birth
- Contact information (phone number, email address, postal address)
- Professional credentials (registration numbers, qualifications, specializations)
- Location data (practice address, territory information, GPS coordinates)
- Financial information (payment details, expense records)
- Professional activity data (visits, prescriptions, sample distributions)
- Biometric data (if applicable)
- Any other information that can identify an individual

"Processing" means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, use, disclosure, combination, restriction, erasure, or destruction.

"Sensitive Personal Data" means Personal Data relating to:

- Passwords and financial information
- Health data
- Biometric data
- Genetic data
- Transgender status
- Caste or tribe
- Religious or political beliefs

3. DATA CONTROLLER AND DATA PROTECTION OFFICER

3.1 Data Fiduciary

Medismo LifeTech(Allied BizTech Solutions Pvt Ltd) acts as the Data Fiduciary for all Personal Data collected and processed through the Services.

Registered Office:
1ST FLOOR, NO.4, WELDER STREET ANNA SALAI , CHENNAI, Tamil Nadu

Corporate Identification Number (CIN): U72900TN2009PTC072281

Email: privacy@medismo.in
Phone: +91 83349 45671

3.2 Data Protection Officer (DPO)

We have appointed a Data Protection Officer to oversee our data protection practices and serve as the point of contact for data-related queries and complaints.

Name: Kumar Dilip M
Designation: Data Protection Officer
Email: dpo@medismo.in
Phone: +91 99625 78801
Business Hours: Monday to Friday, 10:00 AM to 6:00 PM IST

The DPO is responsible for:

- Ensuring compliance with the DPDP Act and this Policy
- Handling data protection queries and complaints
- Coordinating with the Data Protection Board of India
- Overseeing data breach response and notification
- Conducting privacy impact assessments
- Training employees on data protection practices

3.3 Grievance Officer

In accordance with the Information Technology Act, 2000, we have also designated a Grievance Officer:

Name: M Jayashree
Email: grievance@medismo.in
Phone: +91 83349 45671

4. INFORMATION WE COLLECT

4.1 Information You Provide Directly

4.1.1 Account Registration Information

When you create an account or register for our Services, we collect:

- Full name
- Email address
- Phone number (mobile and alternate)
- Company/Organization name
- Job title and role
- Employee ID (if applicable)
- Date of birth
- Professional credentials (medical registration number, pharmaceutical license)
- Username and password (encrypted)
- Profile photograph (optional)

4.1.2 Healthcare Professional Information (FieldVoice)

For doctors, specialists, and healthcare professionals:

- Full name and qualifications (MBBS, MD, MS, etc.)
- Specialization and sub-specialization
- Medical Council registration number (e.g., MCI, State Medical Council)
- Practice locations (hospital/clinic name, address, coordinates)
- Contact details (phone, email, WhatsApp)
- Preferred visiting days and times
- Average patient footfall
- Areas of clinical interest
- Prescribing patterns (aggregated, anonymized)
- Sample distribution records
- Visit history and feedback
- Professional ratings (internal, based on engagement metrics)

Consent Mechanism: We obtain explicit written or digital consent from healthcare professionals before collecting and processing their data, as required under DPDP Act Section 6. Consent forms specify:

- Purpose of data collection
- Types of data collected
- Duration of data retention
- Right to withdraw consent
- Method of consent withdrawal

4.1.3 Patient Information (CareConnect AI & PatientVoice Pro)

IMPORTANT: We do NOT directly collect patient data. Healthcare providers using our Services are responsible for obtaining patient consent. We process patient data only as a Data Processor on behalf of healthcare providers (Data Fiduciaries).

Patient data processed (by healthcare providers) may include:

- Name, age, gender
- Contact information
- Appointment history
- Visit records
- Care pathway status
- Risk scores (calculated by AI, not medical diagnoses)
- Feedback and satisfaction ratings
- Communication preferences
- Language preferences

Legal Basis: Processing of patient data is based on:

- Explicit consent obtained by the healthcare provider
- Legitimate interest in providing healthcare services
- Contractual necessity for service delivery
- Compliance with legal obligations under Clinical Establishments Act and NABH standards

4.1.4 Expense and Financial Information (FieldVoice)

- Expense claims (travel, accommodation, meals)
- Receipt uploads (images)
- Mileage records
- Bank account details (for reimbursement)
- GST information

4.1.5 Communication and Feedback

- Customer support queries and correspondence
- Feedback forms and survey responses
- Chat transcripts and voice recordings (with consent)
- Email communications
- WhatsApp messages (where applicable)

4.2 Information Collected Automatically

4.2.1 Device and Technical Information

- Device type, model, and operating system
- Browser type and version
- IP address
- Device identifiers (IMEI, UDID, Android ID)
- Screen resolution and display settings
- Network information (carrier, connection type)
- App version and build number

4.2.2 Usage and Activity Data

- Pages visited and features used
- Time spent on each page/feature
- Click patterns and navigation paths
- Search queries
- Feature adoption metrics
- Error logs and crash reports
- API call logs

4.2.3 Location Information

- **Precise Location (GPS):** Real-time location data for field force tracking (FieldVoice)
    - Collected only when app is in use (foreground and background with explicit permission)
    - Used for geo-fencing, visit verification, territory mapping
    - Can be disabled, but may limit functionality
- **Approximate Location (IP-based):** Inferred from IP address for analytics
- **Practice Locations:** Manually entered addresses of doctors/hospitals

Consent for Location: We obtain explicit consent before accessing device location services. Users can revoke location permissions through device settings at any time.

4.2.4 Voice Data (FieldVoice)

- Voice recordings for voice-to-text conversion
- Audio snippets for visit reporting
- Voice commands (processed locally on device or via encrypted API)
- Language preferences

Voice Data Handling:

- Voice recordings are processed and deleted immediately after transcription
- No voice data is stored beyond 24 hours
- Users can opt out of voice features
- Transcriptions are stored as text, not audio

4.3 Information from Third Parties

4.3.1 Healthcare Providers

- Employee lists and organizational structures
- Doctor empanelment data
- Hospital information systems (HIS) data (with appropriate data processing agreements)

4.3.2 Pharmaceutical Companies

- Medical representative rosters
- Territory and beat plans
- Product information
- Sample inventory data

4.3.3 Public Sources

- Medical Council registries (for verification)
- Pharmaceutical licensing databases
- Public hospital directories
- Academic and research publications

4.3.4 Business Partners and Vendors

- Payment processors (transaction data)
- Cloud service providers (infrastructure and hosting data)
- Analytics platforms (usage and performance metrics)
- Communication services (email delivery, SMS status)

4.4 Cookies and Tracking Technologies

We use cookies, web beacons, pixels, and similar technologies to:

- Maintain user sessions and authentication
- Remember user preferences and settings
- Analyze usage patterns and improve Services
- Deliver personalized content and recommendations
- Measure marketing campaign effectiveness

Types of Cookies:

1. **Essential Cookies:** Required for basic functionality (cannot be disabled)
2. **Performance Cookies:** Collect anonymous usage data (can be disabled)
3. **Functional Cookies:** Remember your preferences (can be disabled)
4. **Analytics Cookies:** Track usage patterns (can be disabled)

Managing Cookies: You can manage cookie preferences through:

- Browser settings (to block all cookies)
- Our cookie consent banner (granular control)
- Cookie management tool in account settings

Third-Party Cookies: We use:

- Google Analytics (analytics)
- Firebase Analytics (app performance)
- Stripe/Razorpay (payment processing)

See Section 14 for detailed information on cookies and tracking.

5. LEGAL BASIS FOR PROCESSING

Under the DPDP Act, 2023, we process Personal Data based on the following legal grounds:

5.1 Consent (Section 6, DPDP Act)

We rely on your explicit, informed, and freely given consent for:

- Processing of healthcare professional data
- Collection of precise location data
- Voice recording and transcription
- Marketing communications
- Data sharing with third parties (where applicable)
- Processing of sensitive personal data

Consent Characteristics:

- Given in clear and plain language
- Specific to each purpose
- Freely given (no negative consequences for refusal)
- Withdrawable at any time
- Recorded and time-stamped

5.2 Legitimate Interest (Section 7, DPDP Act)

We process Personal Data based on legitimate interests for:

- Service delivery and improvement
- System security and fraud prevention
- Internal analytics and business intelligence
- Customer support and relationship management
- Compliance with legal and regulatory obligations

We ensure that our legitimate interests do not override your fundamental rights and freedoms.

5.3 Contractual Necessity (Section 7, DPDP Act)

Processing is necessary for:

- Performance of contracts with customers
- Taking steps at your request prior to entering a contract
- Service provisioning and billing
- Account management and authentication

5.4 Legal Obligation (Section 7, DPDP Act)

We process Personal Data to comply with:

- Tax laws and financial regulations
- Healthcare regulations (Clinical Establishments Act, Drugs & Cosmetics Act)
- Pharmaceutical marketing codes (UCPMP)
- Court orders and legal process
- Regulatory reporting requirements

5.5 Vital Interest (Section 7, DPDP Act)

In rare cases, processing may be necessary to protect:

- Life or health of a Data Principal
- Public health emergencies
- Critical medical situations

6. PURPOSE AND USE OF INFORMATION

We use your Personal Data for the following purposes:

6.1 Service Delivery and Operations

CareConnect AI

- **Patient Journey Management:** Track and optimize patient care pathways
- **Predictive Analytics:** Generate risk scores and intervention recommendations
- **Appointment Management:** Schedule, reschedule, and send reminders
- **Multi-language Communication:** Send automated messages in 22+ Indian languages
- **Care Coordination:** Connect patients with healthcare providers across departments
- **Readmission Prevention:** Identify high-risk patients and trigger interventions
- **HIS/EMR Integration:** Sync data with hospital information systems

PatientVoice Pro

- **Feedback Aggregation:** Collect and consolidate patient feedback from multiple sources
- **Sentiment Analysis:** Analyze feedback in 10+ languages using AI
- **Trust Scoring:** Calculate department and doctor-level trust scores
- **Reputation Monitoring:** Real-time alerts for negative feedback
- **NABH/HIPAA Reporting:** Generate compliance-ready reports
- **Benchmarking:** Compare performance against industry standards

FieldVoice

- **Field Force Management:** Track medical representative activities and visits
- **Voice Reporting:** Convert voice inputs to structured data in 9 Indian languages
- **Doctor Relationship Management:** Maintain doctor profiles and interaction history
- **Territory Optimization:** Use AI to optimize beat plans and routes
- **Sample Management:** Track sample distribution and acknowledgments
- **Expense Management:** Process and approve expense claims
- **Offline Operations:** Enable full functionality without internet connectivity
- **Compliance Tracking:** Monitor adherence to DGHS/MCI guidelines and UCPMP
- **RCPA Analysis:** Retail chemist prescription audit and competitive intelligence
- **Tour Planning:** Create, approve, and manage monthly tour plans

6.2 Communication and Engagement

- Send transactional notifications (account updates, password resets)
- Deliver appointment reminders and follow-up messages
- Provide customer support and respond to queries
- Share product updates and new feature announcements
- Send training materials and onboarding content
- Conduct surveys and request feedback

6.3 Analytics and Improvement

- Analyze usage patterns and user behavior
- Measure feature adoption and engagement
- Conduct A/B testing and experimentation
- Generate business intelligence and insights
- Improve AI/ML models and algorithms
- Optimize user interface and user experience
- Identify and fix bugs and technical issues

6.4 Security and Fraud Prevention

- Detect and prevent unauthorized access
- Monitor for suspicious activity and anomalies

- Implement risk-based authentication
- Conduct security audits and vulnerability assessments
- Investigate and respond to security incidents
- Maintain audit logs and access records

6.5 Legal and Compliance

- Comply with tax laws and financial regulations
- Respond to legal process (subpoenas, court orders)
- Enforce our Terms of Service and policies
- Protect our rights, property, and safety
- Maintain records for regulatory inspections
- Generate compliance reports (NABH, HIPAA, DGHS)

6.6 Marketing and Promotion (With Consent)

- Send promotional emails and SMS (with opt-out option)
- Display targeted advertisements
- Conduct marketing campaigns
- Measure campaign effectiveness
- Share case studies and success stories (anonymized)

Marketing Consent: You can opt out of marketing communications at any time by:

- Clicking "Unsubscribe" in emails
- Replying "STOP" to SMS messages
- Updating preferences in account settings
- Contacting our DPO at dpo@medismo.in

7. DATA SHARING AND DISCLOSURE

7.1 General Principles

We do not sell, rent, or trade your Personal Data to third parties for their marketing purposes. We share Personal Data only in the following limited circumstances:

7.2 Within Medismo

- Between different product teams (on a need-to-know basis)
- With employees and contractors bound by confidentiality obligations
- With our subsidiaries and affiliates (if any, subject to this Policy)

7.3 With Your Consent

- When you explicitly authorize sharing with third parties
- For specific features that require third-party integration
- When you participate in co-branded offerings

7.4 Service Providers and Data Processors

We engage trusted third-party service providers to perform functions on our behalf, including:

Infrastructure and Hosting

- **Google Cloud Platform / Firebase:** Cloud infrastructure, database, storage, analytics
    - **Location:** Data stored in asia-south1 (Mumbai) region
    - **DPA Status:** Data Processing Agreement in place
    - **Certifications:** ISO 27001, SOC 2 Type II

Communication Services

- **Twilio / MSG91:** SMS and WhatsApp messaging
- **SendGrid / Amazon SES/ Mailgun:** Email delivery
- **Exotel:** Voice calling services

Payment Processing

- **Razorpay / Stripe:** Payment gateway and transaction processing
    - **PCI-DSS Compliant:** Level 1 certification
    - **Data Shared:** Only transaction data, not full payment card details

Analytics and Performance

- **Google Analytics:** Web and app analytics (anonymized IP addresses)
- **Mixpanel:** Product analytics and user behavior
- **Sentry:** Error tracking and crash reporting

Customer Support

- **Freshdesk / Zendesk / OSticket:** Support ticket management
- **Intercom:** In-app chat and customer engagement

Artificial Intelligence

- **OpenAI / Google Cloud AI:** Natural language processing and sentiment analysis
    - **Data Processing:** Anonymized data only
    - **No Training:** Your data is NOT used to train AI models

Data Processor Obligations: All service providers:

- Are contractually bound to process data only per our instructions
- Implement appropriate security measures
- Do not use data for their own purposes
- Delete data upon contract termination
- Comply with the DPDP Act and applicable laws

7.5 Healthcare Providers and Pharmaceutical Companies

- **With Healthcare Providers:** We share aggregated, anonymized patient insights with hospitals and clinics using CareConnect AI and PatientVoice Pro
- **With Pharma Companies:** FieldVoice shares field force performance data with pharmaceutical companies (employers of medical representatives)
- **Doctor Data:** We do NOT share individual doctor data with pharma companies without explicit consent

7.6 Legal and Regulatory Authorities

We may disclose Personal Data to government authorities, regulators, or law enforcement when:

- Required by law, regulation, or legal process (subpoena, court order)
- Necessary to comply with regulatory reporting (e.g., DGHS, State Medical Councils)
- Responding to lawful requests by public authorities (tax, law enforcement)
- Necessary to protect our rights, property, or safety
- Investigating suspected fraud, security incidents, or policy violations

Government Requests: We will:

- Verify the legal validity of the request
- Notify you unless legally prohibited
- Challenge overbroad or improper requests
- Disclose only the minimum necessary data

7.7 Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy, or sale of assets, Personal Data may be transferred to the successor entity, provided:

- The successor agrees to honor this Policy
- You are notified of the transfer
- You have the option to delete your data before transfer

7.8 Aggregated and Anonymized Data

We may share aggregated, anonymized data that does not identify individuals with:

- Research institutions for public health studies
- Industry partners for benchmarking
- Investors and stakeholders for business reporting
- The public via reports, case studies, or publications

Anonymization Standards: We apply technical measures to ensure data cannot be re-identified, including:

- Removal of direct identifiers (name, contact, ID numbers)
- Aggregation (minimum group size of 50)
- Generalization (age ranges, location approximations)
- Noise addition (statistical perturbation)

7.9 Public Forums

If you post content in public areas of our Services (e.g., forums, comment sections), that information is publicly visible and not subject to this Policy.

8. INTERNATIONAL DATA TRANSFERS

8.1 Primary Data Storage

All Personal Data is primarily stored and processed within India, specifically in:

- **Primary Region:** Asia-South1 (Mumbai, India) - Google Cloud Platform
- **Backup Region:** Asia-Southeast1 (Singapore) - for disaster recovery only

8.2 Cross-Border Transfers

In limited circumstances, Personal Data may be transferred outside India to:

- **United States:** For AI/ML processing (OpenAI, Google Cloud AI)
- **Singapore:** For backup and disaster recovery
- **European Union:** For customers using EU-based data centers (if applicable)

8.3 Safeguards for International Transfers

When Personal Data is transferred outside India, we implement appropriate safeguards:

Standard Contractual Clauses (SCCs)

- Legally binding data transfer agreements with recipients
- Based on EU Standard Contractual Clauses (adapted for India)

- Enforceable rights for Data Principals

Adequacy Determinations

- We rely on adequacy decisions by the Government of India (when available)
- Transfer to countries recognized as providing adequate data protection

Explicit Consent

- For transfers not covered by above mechanisms, we obtain explicit consent
- Consent clearly explains the destination country and risks
- Right to withdraw consent at any time

Data Processing Agreements (DPAs)

- All international processors sign DPAs committing to:
    - Process data only per our instructions
    - Implement security measures equivalent to Indian standards
    - Not use data for own purposes
    - Delete data upon contract termination
    - Notify us of data breaches within 24 hours

8.4 Your Rights Regarding International Transfers

- Right to object to international data transfers
- Right to request data be processed only within India
- Right to withdraw consent for cross-border transfers

To Exercise Rights: Contact dpo@medismo.in with subject line "International Transfer Objection"

8.5 HIPAA-Specific Provisions (If Applicable)

If you are a U.S. healthcare provider subject to HIPAA:

- We act as a Business Associate
- A separate Business Associate Agreement (BAA) is executed
- Protected Health Information (PHI) is stored in HIPAA-compliant infrastructure
- Google Cloud Platform BAA covers cloud storage and processing

8.6 GDPR-Specific Provisions (If Applicable)

If you are in the European Economic Area (EEA):

- We act as a Data Controller or Data Processor (as applicable)
- EU Standard Contractual Clauses apply

- Additional rights under GDPR (see Appendix A)
- EU Representative: (information available if required)

9. DATA SECURITY MEASURES

9.1 Security Commitment

We implement industry-leading technical, administrative, and physical safeguards to protect Personal Data against unauthorized access, disclosure, alteration, or destruction.

9.2 Technical Security Measures

9.2.1 Encryption

- **Data in Transit:** TLS 1.3 encryption for all data transmitted over networks
- **Data at Rest:** AES-256 encryption for data stored in databases and file systems
- **End-to-End Encryption:** For voice recordings and sensitive communications
- **Encryption Key Management:** AWS KMS / Google Cloud KMS with regular key rotation

9.2.2 Access Controls

- **Multi-Factor Authentication (MFA):** Required for all admin and privileged accounts
- **Role-Based Access Control (RBAC):** Least-privilege principle applied to all users
- **IP Whitelisting:** Restrict access from authorized IP addresses only
- **Session Management:** Automatic logout after 15 minutes of inactivity
- **Password Policies:** Minimum 12 characters, complexity requirements, 90-day expiration

9.2.3 Network Security

- **Firewalls:** Web Application Firewall (WAF) to block malicious traffic
- **Intrusion Detection:** Real-time monitoring for suspicious activity
- **DDoS Protection:** Cloudflare / Google Cloud Armor to mitigate attacks
- **Network Segmentation:** Isolation of production, staging, and development environments
- **VPN Required:** For remote access to internal systems

9.2.4 Application Security

- **Secure Coding Practices:** OWASP Top 10 guidelines followed
- **Input Validation:** All user inputs sanitized to prevent injection attacks

- **Security Testing:** Automated vulnerability scanning (daily) and manual penetration testing (quarterly)
- **Dependency Management:** Regular updates to patch known vulnerabilities
- **Bug Bounty Program:** Rewards for responsible disclosure of security issues

9.2.5 Database Security

- **Encrypted Backups:** Daily automated backups encrypted with AES-256
- **Backup Retention:** 30-day retention with off-site storage
- **Database Auditing:** All queries logged and monitored for anomalies
- **Principle of Least Privilege:** Database access granted on a need-to-know basis
- **SQL Injection Prevention:** Parameterized queries and prepared statements

9.2.6 Mobile and Offline Security

- **Device Encryption:** Mandatory encryption for FieldVoice mobile app data
- **Secure Storage:** iOS Keychain / Android Keystore for sensitive data
- **Biometric Authentication:** Fingerprint / Face ID for app access (optional)
- **Remote Wipe:** Ability to remotely erase data from lost/stolen devices
- **Offline Data Protection:** Encrypted local storage for offline functionality

9.3 Administrative Security Measures

9.3.1 Employee Training

- Mandatory data privacy and security training for all employees (annually)
- Role-specific training (e.g., developers, support, sales)
- Phishing awareness and social engineering prevention
- Incident response drills and tabletop exercises

9.3.2 Background Checks

- Criminal background checks for all employees with access to Personal Data
- Reference verification and employment history checks
- Ongoing monitoring for insider threats

9.3.3 Confidentiality Agreements

- All employees, contractors, and vendors sign Non-Disclosure Agreements (NDAs)
- Contractual obligations to protect Personal Data
- Penalties for unauthorized disclosure

9.3.4 Access Audits

- Quarterly reviews of user access privileges
- Annual recertification of access by managers

- Immediate revocation of access upon termination

9.3.5 Change Management

- All code changes reviewed before deployment
- Approval workflow for infrastructure changes
- Version control and rollback capabilities

9.4 Physical Security Measures

- **Data Center Security:** ISO 27001 certified facilities with 24/7 monitoring
- **Access Control:** Biometric authentication and mantrap entrances
- **Surveillance:** CCTV cameras with 90-day retention
- **Environmental Controls:** Fire suppression, climate control, backup power (UPS, generators)
- **Secure Disposal:** Degaussing and physical destruction of retired hardware

9.5 Vendor Security Management

- Security assessments of all third-party vendors
- Contractual security requirements in all agreements
- Regular audits and compliance reviews
- Annual security questionnaires (SOC 2, ISO 27001)

9.6 Incident Response and Business Continuity

9.6.1 Security Incident Response Plan

- **Detection:** 24/7 security monitoring and alerting
- **Containment:** Immediate isolation of affected systems
- **Investigation:** Forensic analysis to determine scope and impact
- **Remediation:** Patch vulnerabilities and restore services
- **Notification:** Inform affected users and authorities within 72 hours (as required by DPDP Act Section 8)

9.6.2 Business Continuity and Disaster Recovery

- **RPO (Recovery Point Objective):** 1 hour (maximum data loss)
- **RTO (Recovery Time Objective):** 4 hours (maximum downtime)
- **Disaster Recovery Plan:** Tested quarterly
- **Geographic Redundancy:** Multi-region failover capabilities
- **Crisis Management Team:** On-call 24/7

9.7 Compliance and Certifications

We maintain the following security certifications and compliance frameworks:

- **ISO 27001:2013** - Information Security Management System (In Progress)
- **SOC 2 Type II** - Security, Availability, Confidentiality (Planned)
- **PCI DSS** - Payment Card Industry Data Security Standard (via Razorpay/Stripe)
- **HIPAA** - Business Associate Agreement available for U.S. healthcare customers
- **NABH** - National Accreditation Board for Hospitals compliance support

9.8 Limitations of Security

Important Notice: While we implement comprehensive security measures, no system is 100% secure. Risks include:

- Zero-day vulnerabilities in third-party software
- Advanced persistent threats (APTs) from nation-state actors
- Insider threats from malicious employees
- Social engineering attacks targeting users
- Force majeure events (natural disasters, war, terrorism)

Your Responsibility: You are responsible for:

- Maintaining confidentiality of your credentials
- Using strong, unique passwords
- Enabling MFA when available
- Not sharing your account with others
- Reporting suspicious activity immediately

10. DATA RETENTION AND DELETION

10.1 Retention Principles

We retain Personal Data only for as long as necessary to fulfill the purposes outlined in this Policy, comply with legal obligations, resolve disputes, and enforce our agreements.

10.2 Retention Periods by Data Type

Data Type	Retention Period	Legal Basis
User Account Data	Duration of account + 3 years	Contractual necessity, legal compliance

Healthcare Professional Data	Duration of consent + 3 years	Consent, legitimate interest
Patient Data (CareConnect AI)	As determined by healthcare provider (typically 5-10 years)	Healthcare provider's legal obligations, medical records laws
Visit Records & DCRs (FieldVoice)	5 years from date of visit	Pharmaceutical industry regulations, tax laws
Expense Records	7 years from fiscal year end	Income Tax Act, 1961
Sample Distribution Records	5 years from distribution date	Drugs & Cosmetics Act, 1940
Prescription Audit Data (RCPA)	3 years from collection	Business intelligence, competitive analysis
Communication Logs (Email, SMS, Voice)	2 years from communication date	Customer service, dispute resolution
Voice Recordings	24 hours (deleted after transcription)	Operational necessity
Location Data (GPS)	90 days from collection	Field force management, compliance
Transaction and Payment Data	7 years from transaction date	Tax laws, financial regulations

Marketing Communications	Until opt-out + 30 days	Consent, marketing compliance
Security Logs and Audit Trails	2 years from creation	Security, forensics, regulatory compliance
Cookie Data	13 months from collection	ePrivacy Directive compliance
Anonymized Analytics Data	Indefinitely	Not Personal Data, business intelligence

10.3 Extended Retention for Legal Purposes

Data may be retained beyond standard periods when:

- Required by law or regulation
- Necessary for pending litigation or investigations
- Subject to legal hold or preservation notice
- Required for tax audits or regulatory inspections
- Necessary to establish, exercise, or defend legal claims

Notification: You will be notified if your data is retained beyond standard periods for legal reasons.

10.4 Deletion and Anonymization

10.4.1 Automatic Deletion

- **Expired Consents:** Data is automatically anonymized within 30 days of consent withdrawal
- **Inactive Accounts:** Accounts inactive for 3+ years receive deletion notice (90-day warning)
- **Temporary Data:** Voice recordings, session data, and temporary files are auto-deleted per schedule

10.4.2 Secure Deletion Methods

- **Database Records:** Multi-pass overwrite (DoD 5220.22-M standard)
- **Backups:** Removed from all backup cycles within 30 days

- **File Storage:** Cryptographic erasure (encryption keys destroyed)
- **Physical Media:** Degaussing and physical shredding (for retired hardware)
- **Third-Party Systems:** Deletion requests sent to all processors within 7 days

10.4.3 Anonymization Standards

When anonymization is used instead of deletion:

- **Irreversibility:** Data cannot be re-identified by any reasonable means
- **Techniques Applied:**
    - Removal of all direct identifiers (name, contact, ID numbers, registration numbers)
    - Generalization (age → age range, exact location → district/state)
    - Aggregation (minimum group size of 50 individuals)
    - Noise addition (statistical perturbation for numeric values)
    - Data masking (partial redaction of identifiers)

10.5 Data Retention

You can view retention schedules for your data by Request a Data Retention Report from dpo@medismo.in

10.6 Early Deletion Requests

You may request early deletion of your data by:

- Submitting a deletion request via Account Settings
- Emailing dpo@medismo.in with subject "Data Deletion Request"
- Contacting our DPO via phone

Processing Time: Deletion requests are processed within 30 days. You will receive confirmation once completed.

Exceptions: We may refuse deletion if:

- Required by law to retain the data
- Necessary for pending litigation or investigations
- Needed to complete a transaction you initiated
- Required for security and fraud prevention
- Necessary to exercise freedom of speech or other legal rights

If deletion is refused, we will provide a written explanation of the reasons.

11. YOUR RIGHTS UNDER DPDP ACT 2023

As a Data Principal under the Digital Personal Data Protection Act, 2023, you have the following rights:

11.1 Right to Access (Section 11, DPDP Act)

You have the right to obtain:

- Confirmation whether your Personal Data is being processed
- Access to your Personal Data in our possession
- Information about the purposes of processing
- Categories of Personal Data being processed
- Recipients or categories of recipients of your data
- Retention period for your data
- Information about data sources (if not collected directly from you)

How to Exercise:

- Login to your account and navigate to Settings → Privacy → Download My Data
- Email dpo@medismo.in with subject "Data Access Request"
- Submit a written request to our registered office

Response Time: Within 30 days of receiving a valid request

Format: Data provided in machine-readable format (CSV, JSON, PDF)

Fee: First request per year is free; subsequent requests may incur a reasonable administrative fee (max ₹1200)

11.2 Right to Correction (Section 12, DPDP Act)

You have the right to:

- Correct inaccurate Personal Data
- Complete incomplete Personal Data
- Update outdated Personal Data

How to Exercise:

- Update information directly in your account settings
- Submit correction request via Account Settings → Privacy → Request Correction
- Email dpo@medismo.in with supporting documentation

Response Time: Corrections processed within 15 days

Verification: We may request verification of your identity and proof of corrections (e.g., updated medical registration, new contact proof)

11.3 Right to Erasure / Right to be Forgotten (Section 12, DPDP Act)

You have the right to request deletion of your Personal Data when:

- Data is no longer necessary for the purposes it was collected
- You withdraw consent (and no other legal basis applies)
- You object to processing and there are no overriding legitimate grounds
- Data has been unlawfully processed
- Data must be erased to comply with a legal obligation

How to Exercise:

- Account Settings → Privacy → Delete My Account
- Email dpo@medismo.in with subject "Data Erasure Request"
- Submit written request with identity verification

Response Time: Deletion completed within 30 days

Limitations: We may refuse or delay deletion if:

- Required by law to retain data (e.g., tax records, medical records)
- Necessary for legal claims or regulatory investigations
- Required for security or fraud prevention
- You have an outstanding financial obligation

Confirmation: You will receive written confirmation once deletion is complete, including details of any data retained for legal reasons.

11.4 Right to Data Portability (Section 12, DPDP Act)

You have the right to:

- Receive your Personal Data in a structured, commonly used, machine-readable format
- Transmit your data to another Data Fiduciary (where technically feasible)

How to Exercise:

- Account Settings → Privacy → Export My Data
- Select format: CSV, JSON, or XML
- Data will be emailed within 24 hours

Scope: Includes data you provided or data generated through your use of Services (does not include inferred or derived data)

Portability Formats:

- **CareConnect AI / PatientVoice Pro:** CSV, JSON
- **FieldVoice:** Excel, CSV, JSON

11.5 Right to Withdraw Consent (Section 6(6), DPDP Act)

You have the right to withdraw consent at any time, where processing is based on consent.

How to Exercise:

- Account Settings → Privacy → Manage Consent
- Toggle off specific consent purposes
- Email dpo@medismo.in with withdrawal request

Effect of Withdrawal:

- We will stop processing your data for the specified purpose
- Data may be retained if another legal basis applies (e.g., legal obligation)
- Withdrawal does not affect lawfulness of processing before withdrawal
- Some features may become unavailable (you will be notified)

Examples:

- Withdraw consent for marketing → No more promotional communications
- Withdraw consent for location tracking → FieldVoice territory features disabled
- Withdraw consent for voice recording → Must use text input instead

11.6 Right to Nominate (Section 13, DPDP Act)

You have the right to nominate another individual to exercise your rights in the event of:

- Your death
- Your incapacity (physical or mental inability)

How to Exercise:

- Account Settings → Privacy → Nominate Representative
- Provide nominee's name, email, phone, and relationship
- Nominee will receive notification and activation code

Nominee's Rights: Can exercise all rights on your behalf, including access, correction, and deletion

Revocation: You can change or revoke nomination at any time

11.7 Right to Grievance Redressal (Section 17, DPDP Act)

You have the right to:

- Lodge a complaint with our Grievance Officer
- Receive acknowledgment within 24 hours
- Receive resolution within 30 days
- Escalate to Data Protection Board of India if unsatisfied

How to Exercise:

- Email grievance@medismo.in
- Use grievance form: https://medismo.in/contact
- Call Grievance Officer at +91 99625-78801
- Written complaint to registered office

See Section 16 for detailed grievance redressal process.

11.8 Right to Object to Processing (Section 12, DPDP Act)

You have the right to object to processing of your Personal Data when:

- Processing is based on legitimate interest
- Processing is for direct marketing purposes
- Processing is for research or statistical purposes

How to Exercise:

- Account Settings → Privacy → Object to Processing
- Specify the processing activity you object to
- Provide reasons for objection (optional)

Our Response:

- We will stop processing unless we can demonstrate compelling legitimate grounds
- You will receive a written explanation of our decision
- If objection is upheld, data will be deleted or anonymized

11.9 Right to Complain to Data Protection Board

If you are dissatisfied with our handling of your Personal Data or our response to your requests, you have the right to lodge a complaint with:

Data Protection Board of India
Before Complaining to DPBI: We encourage you to contact our DPO first to resolve the issue amicably.

11.10 Exercising Your Rights

Identity Verification: To protect your privacy, we will verify your identity before processing requests. You may be asked to provide:

- Government-issued photo ID (Aadhaar, PAN, Passport, Driving License)
- Proof of email address or phone number
- Security questions or account verification code

Authorized Representatives: You may authorize another person to exercise rights on your behalf by:

- Providing written authorization (signed and dated)
- Submitting proof of representative's identity
- Specifying scope of authorization

No Retaliation: We will not discriminate against you for exercising your rights. Your services will not be denied, degraded, or made more expensive.

Response Timeline:

- Acknowledgment: Within 72 hours
- Resolution: Within 30 days (may be extended by 30 days for complex requests)
- If extension needed, you will be notified with reasons

12. CHILDREN'S PRIVACY

12.1 Age Restriction

Our Services are NOT intended for individuals under the age of 18 years ("**Children**" or "**Minors**").

12.2 No Knowing Collection

We do not knowingly collect, process, or solicit Personal Data from Children. If you are under 18, please do not:

- Register for an account
- Use our Services
- Provide any Personal Data to us

12.3 Parental Consent (Section 9, DPDP Act)

If we need to process a Child's Personal Data for a legitimate purpose (e.g., child patients in CareConnect AI), we will:

- Obtain verifiable parental consent before collection
- Use age-appropriate language in consent notices
- Allow parents to review, modify, or delete their child's data
- Implement heightened security measures for children's data
- Limit data collection to the minimum necessary

Parental Rights:

- Access child's Personal Data
- Request correction or deletion
- Withdraw consent at any time
- Prevent further processing

12.4 Verification of Parental Consent

For child patients (CareConnect AI), parental consent is verified through:

- Parent's signature on hospital consent forms
- Parent's verified mobile number or email
- In-person verification at healthcare facility

12.5 Inadvertent Collection

If we discover that we have inadvertently collected Personal Data from a Child without proper consent:

- We will delete the data immediately (within 24 hours)
- We will notify the parent/guardian (if contact information is available)
- We will document the incident for compliance records

12.6 Reporting Concerns

If you believe we have collected Personal Data from a Child without proper consent, please contact us immediately:

- Email: dpo@medismo.in
- Phone: +91 83349 45671
- Subject: "Child Privacy Concern"

13. COOKIES AND TRACKING TECHNOLOGIES

13.1 What Are Cookies?

Cookies are small text files stored on your device (computer, smartphone, tablet) when you visit our websites or use our web-based Services. They help us recognize your device and remember your preferences.

13.2 Types of Cookies We Use

13.2.1 Essential Cookies (Strictly Necessary)

Purpose: Enable basic functionality and security **Examples:**

- Session authentication tokens
- Load balancing and routing
- Security and fraud prevention
- CSRF protection

Can Be Disabled? No – these are required for Services to function

Duration: Session cookies (deleted when browser closed) or up to 1 year

13.2.2 Performance Cookies (Analytics)

Purpose: Understand how users interact with our Services **Examples:**

- Page views and navigation paths
- Feature usage and adoption
- Error rates and performance metrics
- A/B testing and experimentation

Third-Party Services:

- Google Analytics (_ga, _gid, _gat)
- Firebase Analytics
- Mixpanel

Can Be Disabled? Yes – through cookie consent banner or browser settings

Duration: Up to 2 years

Opt-Out:

- Cookie Settings in footer
- Google Analytics Opt-Out: https://tools.google.com/dlpage/gaoptout

13.2.3 Functional Cookies (Preference)

Purpose: Remember your preferences and settings **Examples:**

- Language preferences
- Theme (light/dark mode)
- Dashboard layout
- Recently viewed items
- Notification preferences

Can Be Disabled? Yes – but some features may not work as expected

Duration: Up to 1 year

13.2.4 Marketing Cookies (Targeting)

Purpose: Deliver relevant advertisements and measure campaign effectiveness **Examples:**

- Google Ads remarketing
- LinkedIn Insight Tag
- Facebook Pixel

Can Be Disabled? Yes – highly recommended if you don't want targeted ads

Duration: Up to 2 years

Opt-Out:

- Cookie Settings in footer
- Network Advertising Initiative: https://optout.networkadvertising.org/
- Digital Advertising Alliance: https://optout.aboutads.info/

13.3 Other Tracking Technologies

13.3.1 Web Beacons (Pixels)

Small transparent images embedded in emails or web pages to track:

- Email open rates
- Click-through rates
- Page visits after clicking email links

Used In: Marketing emails, web pages, advertisements

13.3.2 Local Storage

Browser-based storage for larger data sets:

- Offline functionality (FieldVoice mobile app)
- Cached data for faster loading
- User preferences and settings

Persistence: Until manually cleared or app uninstalled

13.3.3 Device Fingerprinting

Collection of device characteristics for fraud prevention:

- Browser type and version
- Operating system
- Screen resolution
- Installed fonts and plugins

Purpose: Security, fraud detection, duplicate account prevention

Not Used For: Tracking across websites or long-term profiling

13.4 Mobile App Tracking

13.4.1 Mobile Advertising IDs

- **Android:** Google Advertising ID (GAID)
- **iOS:** Identifier for Advertisers (IDFA)

Purpose: Analytics and attribution (if you opt-in to tracking)

How to Disable:

- **Android:** Settings → Google → Ads → Reset advertising ID or Opt out of Ads Personalization
- **iOS:** Settings → Privacy & Security → Tracking → Disable "Allow Apps to Request to Track"

13.4.2 Push Notification Tokens

- Device-specific tokens for sending push notifications
- Not used for tracking; solely for notification delivery
- Can be disabled in device settings

13.5 Managing Cookies and Tracking

13.5.1 Cookie Consent Banner

On first visit, you will see a cookie consent banner allowing you to:

- Accept all cookies
- Reject non-essential cookies
- Customize cookie preferences (granular control)

Re-accessing Settings: Click "Cookie Settings" in website footer at any time

13.5.2 Browser Settings

You can manage cookies through your browser:

- **Chrome:** Settings → Privacy and security → Cookies and other site data
- **Firefox:** Settings → Privacy & Security → Cookies and Site Data
- **Safari:** Preferences → Privacy → Manage Website Data
- **Edge:** Settings → Cookies and site permissions

Note: Blocking all cookies may prevent Services from functioning properly.

13.5.3 Do Not Track (DNT)

We currently do not respond to Do Not Track browser signals, as there is no industry consensus on how to interpret DNT. However, you can control tracking through:

- Cookie consent settings
- Browser cookie settings
- Opt-out tools listed above

13.6 Third-Party Cookies

Our websites may contain links to third-party websites (e.g., social media, payment processors). These third parties may set their own cookies, which are governed by their privacy policies, not ours.

We Are Not Responsible For:

- Third-party cookie practices
- Data collected by third parties
- Third-party privacy policies

Review Third-Party Policies:

- Google Privacy Policy: https://policies.google.com/privacy
- Facebook Data Policy: https://www.facebook.com/privacy/policy
- LinkedIn Privacy Policy: https://www.linkedin.com/legal/privacy-policy

13.7 Cookie Retention

Cookies are retained for the following periods:

- **Session Cookies:** Deleted when browser is closed
- **Persistent Cookies:** Remain until expiration date or manual deletion

- **Maximum Duration:** 2 years (in compliance with ePrivacy Directive)

13.8 Updates to Cookie Usage

If we introduce new cookies or tracking technologies, we will:

- Update this section of the Privacy Policy
- Notify you via email or in-app notification (for material changes)
- Request renewed consent (if required by law)

14. THIRD-PARTY LINKS AND SERVICES

14.1 Third-Party Links

Our Services may contain links to external websites, applications, or services operated by third parties, including:

- Social media platforms (LinkedIn, Facebook, Twitter)
- Payment gateways (Razorpay, Stripe)
- Educational content and research papers
- Partner integrations (HIS/EMR systems, communication platforms)

14.2 No Endorsement

Inclusion of third-party links does not imply endorsement, approval, or recommendation by Medismo. We are not responsible for:

- Content, accuracy, or practices of third-party websites
- Privacy policies or terms of service of third parties
- Security of third-party platforms
- Data collected by third parties

14.3 Your Responsibility

Before interacting with third-party services:

- Review their privacy policies and terms of service
- Understand what data they collect and how they use it
- Assess security and trustworthiness
- Exercise caution when providing Personal Data

14.4 Third-Party Integrations

Some features require integration with third-party services (e.g., hospital HIS/EMR systems, WhatsApp Business API). When using such features:

- You explicitly consent to data sharing with the third party
- Data shared is limited to what's necessary for the integration
- Third parties are contractually bound to protect your data
- You can disable integrations at any time in account settings

14.5 Social Media Plugins

Our websites may include social media plugins (e.g., "Share" buttons). When you interact with these plugins:

- Your IP address and page visited may be shared with the social media platform
- If logged into the social platform, they may link your visit to your profile
- Social media platforms may set cookies on your device

To Prevent Tracking: Log out of social media platforms before visiting our site, or use browser privacy modes.

15. CHANGES TO PRIVACY POLICY

15.1 Right to Modify

We reserve the right to modify, update, or replace this Privacy Policy at any time to reflect:

- Changes in our data practices
- New features or Services
- Legal, regulatory, or compliance requirements
- Industry best practices
- User feedback

15.2 Notification of Changes

Material Changes

For significant changes that expand our data processing practices or reduce your rights, we will:

- Notify you via email (to your registered email address)
- Display a prominent in-app notification
- Request renewed consent (if required by law)
- Provide 30 days' notice before changes take effect

Examples of Material Changes:

- Introducing new data collection practices
- Sharing data with new categories of third parties
- Transferring data to new countries
- Changes to data retention periods

Non-Material Changes

For minor updates (e.g., clarifications, formatting, contact information), we will:

- Post the updated Policy on our website
- Update the "Last Updated" date at the top
- No prior notice required

15.3 Acceptance of Changes

By continuing to use our Services after the updated Policy takes effect, you acknowledge and agree to the changes. If you do not agree with the changes:

- You may stop using our Services
- You may request deletion of your account and data
- We will honor your deletion request within 30 days

15.4 Version History

We maintain a version history of all Privacy Policy changes:

- Accessible at: medismo.in/privacy-policy-archive
- Shows previous versions and change logs
- Available for review at any time

15.5 Periodic Review

We review this Privacy Policy at least annually to ensure continued compliance with:

- DPDP Act, 2023
- Evolving data protection laws
- Industry standards
- Best practices

Last Full Review: Oct, 2025

Next Scheduled Review: Oct 2026

16. GRIEVANCE REDRESSAL MECHANISM

16.1 Overview

In accordance with Section 17 of the DPDP Act, we have established a robust grievance redressal mechanism to address your data protection concerns.

16.2 Grievance Officer

Name: Kumar Dilip M
Designation: Grievance Officer
Email: grievance@medismo.in
Phone: +91-8334945671
Address: 1ST FLOOR, NO.4, WELDER STREET, ANNA SALAI, Chennai, Tamil Nadu, 600002
Business Hours: Monday to Friday, 10:00 AM to 6:00 PM IST

16.3 Scope of Grievances

You may file a grievance regarding:

- Unauthorized collection or processing of Personal Data
- Refusal to honor data rights (access, correction, deletion)
- Data breach or security incidents
- Lack of transparency in data practices
- Non-compliance with this Privacy Policy
- Misuse or unauthorized disclosure of Personal Data
- Failure to respond to data requests within timelines
- Any other data protection concern

16.4 How to File a Grievance

Step 1: Submit Grievance

Choose one of the following methods:

- **Email:** grievance@medismo.in (Subject: "Grievance - [Brief Description]")
- **Phone:** +91-[INSERT PHONE] (call during business hours)
- **Mail:** Written complaint to registered office address

Step 2: Provide Details

Include the following information:

- Your full name and contact details (email, phone)
- User ID or account email (if applicable)

- Description of the grievance (be specific)
- Date and time of incident (if applicable)
- Steps already taken to resolve (e.g., contacted support)
- Supporting documents (screenshots, emails, etc.)
- Preferred resolution or outcome

Step 3: Identity Verification

For security, we may request:

- Government-issued photo ID
- Account verification code (sent to registered email/phone)
- Security questions

16.5 Grievance Handling Process

Acknowledgment (Within 24 Hours)

You will receive an acknowledgment containing:

- Unique grievance reference number (format: GRV-YYYY-XXXXX)
- Name of assigned investigator
- Expected resolution timeline
- Contact details for follow-up

Investigation (Within 15 Days)

Our team will:

- Review your grievance and supporting evidence
- Investigate relevant systems, logs, and records
- Contact you for additional information (if needed)
- Consult with relevant teams (engineering, legal, security)
- Prepare a detailed investigation report

Resolution (Within 30 Days)

You will receive a written response containing:

- Summary of investigation findings
- Explanation of our determination
- Corrective actions taken (if applicable)
- Steps to prevent recurrence
- Your rights to escalate (if dissatisfied)

Timeline Extension: Complex grievances may require up to 60 days. You will be notified of any extension with reasons.

16.6 Escalation

Internal Escalation

If you are dissatisfied with the Grievance Officer's response:

- **Escalate To:** Data Protection Officer (DPO)
- **Email:** dpo@medismo.in
- **Timeline:** DPO will review within 15 days
- **Final Internal Decision:** DPO's decision is final internally

External Escalation

If still dissatisfied after internal escalation, you may:

- **File Complaint With:** Data Protection Board of India
- **Timeline:** As per DPBI procedures
- **Representation:** You may engage legal counsel

16.7 Grievance Tracking

Track your grievance status:

- **Email:** Grievance reference number and registered email to know the status updates and investigator notes

Status Types:

- Received: Grievance submitted and acknowledged
- Under Investigation: Team is reviewing the matter
- Pending Information: Waiting for additional details from you
- Resolved: Grievance closed with resolution
- Escalated: Forwarded to DPO or senior management

16.8 No Retaliation

We strictly prohibit retaliation against individuals who file grievances in good faith. Your:

- Services will not be terminated or degraded
- Account will not be penalized
- Pricing will not be increased
- Support will not be deprioritized

If You Experience Retaliation: Report immediately to dpo@medismo.in

16.9 Grievance Statistics

We publish quarterly grievance statistics:

- Total grievances received
- Categories of grievances
- Average resolution time
- Percentage resolved in favor of complainant
- Lessons learned and process improvements

17. CONTACT INFORMATION

17.1 Data Fiduciary

Medismo LifeTech(Allied BizTech Solutions Pvt Ltd) acts as the Data Fiduciary for all Personal Data collected and processed through the Services.

Registered Office:
1ST FLOOR, NO.4, WELDER STREET ANNA SALAI , CHENNAI, Tamil Nadu

Corporate Identification Number (CIN): U72900TN2009PTC072281

Email: privacy@medismo.in
Phone: +91 83349 45671

17.2 Data Protection Officer (DPO)

We have appointed a Data Protection Officer to oversee our data protection practices and serve as the point of contact for data-related queries and complaints.

Name: Kumar Dilip M
Designation: Data Protection Officer
Email: dpo@medismo.in
Phone: +91 99625 78801
Business Hours: Monday to Friday, 10:00 AM to 6:00 PM IST

The DPO is responsible for:

- Ensuring compliance with the DPDP Act and this Policy
- Handling data protection queries and complaints
- Coordinating with the Data Protection Board of India
- Overseeing data breach response and notification
- Conducting privacy impact assessments

- Training employees on data protection practices

17.3 Grievance Officer

In accordance with the Information Technology Act, 2000, we have also designated a Grievance Officer:

Name: M Jayashree
Email: grievance@medismo.in
Phone: +91 83349 45671

17.4 General Inquiries

Customer Support: support@medismo.in
Sales: sales@medismo.in
Partnerships: partnerships@medismo.in
Media: media@medismo.in

17.5 Business Hours

Monday to Friday: 10:00 AM to 6:00 PM IST
Saturday: 10:00 AM to 2:00 PM IST (Support only)
Sunday: Closed

Emergency Contact (Data Breach): Available 24/7 at security@medismo.in

PART B: TERMS OF SERVICE

1. ACCEPTANCE OF TERMS

1.1 Agreement to Terms

These Terms of Service ("**Terms**," "**Agreement**," or "**TOS**") constitute a legally binding agreement between you ("**User**," "**you**," or "**your**") and Medismo Healthcare Technologies Private Limited ("**Medismo**," "**we**," "**us**," or "**our**") governing your access to and use of our Services.

1.2 Scope of Application

These Terms apply to:

- CareConnect AI (Patient Journey Intelligence Platform)

- PatientVoice Pro (Patient Trust Intelligence Platform)
- FieldVoice (Voice-Powered Pharma CRM)
- All associated websites, mobile applications, APIs, and software (collectively, "**Services**")

1.3 Acceptance

By accessing, registering for, or using our Services, you:

- Acknowledge that you have read, understood, and agree to be bound by these Terms
- Agree to comply with all applicable laws and regulations
- Confirm that you have the legal authority to enter into this Agreement
- Accept our Privacy Policy (incorporated herein by reference)

If you do not agree to these Terms, you must not access or use our Services.

1.4 Electronic Acceptance

Your electronic acceptance (clicking "I Agree," "Accept," or similar buttons) constitutes a valid and enforceable electronic signature under the Information Technology Act, 2000.

1.5 Organizational Authority

If you are accepting these Terms on behalf of an organization:

- You represent and warrant that you have the authority to bind the organization
- The organization accepts these Terms and is responsible for your actions
- "You" refers to both you as an individual and the organization

2. SERVICE DESCRIPTION

2.1 CareConnect AI

Features

- **Patient Journey Intelligence:** Track patient care pathways across touchpoints
- **Predictive AI Engine:** Identify at-risk patients and predict appointment no-shows
- **Automated Care Orchestration:** Trigger interventions based on patient behavior
- **Multilingual Communication:** Send messages in 22+ Indian languages
- **Risk Scoring:** Real-time patient risk assessment and prioritization
- **HIS/EMR Integration:** Seamless integration with hospital information systems
- **Appointment Management:** Scheduling, reminders, and no-show reduction
- **Readmission Prevention:** Identify and engage high-risk post-discharge patients

Intended Users

- Hospitals and healthcare facilities
- Clinics and nursing homes
- Diagnostic centers
- Healthcare administrators

Service Level

- **Uptime:** 99.5% (excluding scheduled maintenance)
- **Support:** Email and phone support during business hours
- **Data Refresh:** Real-time for transactional data, daily for analytics

2.2 PatientVoice Pro

Features

- **Multi-Source Feedback Aggregation:** Collect from surveys, social media, calls, emails
- **AI Sentiment Analysis:** Analyze feedback in 10+ Indian languages
- **Trust Scoring:** Department and doctor-level trust metrics
- **Reputation Shield:** Real-time alerts for negative feedback
- **NABH/HIPAA Compliance:** Generate compliance-ready reports
- **Benchmarking:** Compare against industry standards
- **Root Cause Analysis:** Identify systemic issues from feedback patterns
- **Action Tracking:** Monitor resolution of patient concerns

Intended Users

- Hospital quality teams
- Patient experience managers
- Healthcare administrators
- NABH accreditation teams

Service Level

- **Uptime:** 99.5%
- **Feedback Processing:** Within 15 minutes of receipt
- **Sentiment Analysis:** Real-time
- **Support:** Email and phone during business hours

2.3 FieldVoice

Features

- **Voice-to-Text Reporting:** DCR submission in Hindi + 8 regional languages
- **Offline Mode:** Full functionality without internet (7-day sync)

- **Doctor Relationship Intelligence:** Comprehensive doctor profiles and visit history
- **Territory Optimization:** AI-powered beat planning and route optimization
- **Sample Management:** Track allocation, distribution, and ROI
- **Expense Management:** Receipt OCR, automated categorization, approval workflows
- **Tour Planning:** Monthly tour plan creation with manager approval
- **RCPA (Retail Chemist Prescription Audit):** Competitive intelligence and market share analysis

DGHS/MCI Compliance Tracking: Monitor adherence to UCPMP and medical council regulations

- **Real-Time Field Tracking:** GPS-based visit verification and geo-fencing
- **WhatsApp Integration:** Doctor engagement via WhatsApp Business API
- **Analytics Dashboard:** Performance metrics, target achievement, territory insights

Intended Users

- Pharmaceutical companies
- Medical representatives (field force)
- Area and regional managers
- Sales operations teams

Service Level

- **Uptime:** 99.5% for cloud services; 100% offline functionality
- **Data Sync:** Real-time when online; automatic sync when connectivity restored
- **Voice Recognition Accuracy:** 95%+ for supported languages
- **Support:** Email, phone, and in-app chat during business hours

2.4 Service Modifications

We reserve the right to:

- Modify, update, or discontinue features or Services (with 30 days' notice for material changes)
- Introduce new features or Services (may require additional fees)
- Conduct scheduled maintenance (announced 48 hours in advance)
- Perform emergency maintenance (without notice if critical)

Material Changes: For significant modifications affecting core functionality, we will:

- Notify you via email and in-app notification
- Provide 30 days' notice before changes take effect
- Allow you to terminate if you do not agree (with pro-rated refund)

2.5 Beta Features

We may offer beta, pilot, or preview features marked as "Beta," "Preview," or "Experimental":

- Provided on an "as-is" basis without warranties
- May be unstable, incomplete, or subject to bugs
- May be modified or discontinued without notice
- Data may not be retained after beta period
- Separate beta terms may apply

Feedback: By using beta features, you agree to provide feedback and allow us to use it without compensation.

3. USER ELIGIBILITY AND REGISTRATION

3.1 Age Requirement

You must be at least 18 years old to use our Services. By using our Services, you represent that you meet this age requirement.

3.2 Legal Capacity

You must have the legal capacity to enter into binding contracts. You represent that:

- You are not legally prohibited from entering into contracts
- You are not subject to any legal disability
- You have not been previously suspended or banned from our Services

3.3 Professional Qualifications

Healthcare Providers (CareConnect AI, PatientVoice Pro)

You must:

- Be a licensed healthcare facility registered under the Clinical Establishments Act, 2010 (or equivalent state law)
- Hold all necessary permits, licenses, and accreditations (e.g., NABH, NABL)
- Employ qualified healthcare professionals as per applicable regulations

Medical Representatives (FieldVoice)

You must:

- Be employed by a licensed pharmaceutical company
- Hold a valid pharmaceutical representative certificate (if required by state)
- Comply with the Uniform Code of Pharmaceutical Marketing Practices (UCPMP)

Healthcare Professionals (FieldVoice - Doctors)

You must:

- Hold a valid medical license from the Medical Council of India or State Medical Council
- Maintain current registration and good standing
- Comply with Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002

3.4 Account Registration

Required Information

To register, you must provide:

- Full legal name
- Valid email address
- Mobile phone number
- Organization name and details
- Professional credentials (license numbers, registration)
- Billing information (for paid Services)

Account Types

- **Individual Account:** For single users (e.g., independent practitioners)
- **Organization Account:** For companies, hospitals, or clinics (with admin and sub-users)
- **Trial Account:** 14-30 day free trial with limited features

Account Credentials

You are responsible for:

- Creating a strong password (minimum 12 characters, mixed case, numbers, special characters)
- Keeping your credentials confidential
- Not sharing your account with others
- Notifying us immediately of unauthorized access (security@medismo.in)

Account Security: We recommend enabling Multi-Factor Authentication (MFA) for enhanced security.

3.5 Account Verification

We may verify your identity and credentials by:

- Sending verification codes to your email or phone

- Requesting copies of professional licenses or registration certificates
- Conducting background checks (for organizational accounts)
- Verifying organizational details (company registration, GST)

Failure to Verify: We may suspend or terminate accounts that fail verification within 30 days.

3.6 One Account Per User

You may maintain only one account per user. Creating multiple accounts (including using different email addresses) is prohibited unless explicitly authorized.

3.7 Account Accuracy

You must:

- Provide accurate, complete, and current information
- Update information promptly when it changes
- Not impersonate any person or entity
- Not misrepresent your affiliation with any organization

Consequences of Inaccurate Information: We may suspend or terminate accounts providing false information.

4. LICENSE AND ACCESS RIGHTS

4.1 Limited License

Subject to your compliance with these Terms, we grant you a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to:

- Access and use the Services for your internal business purposes
- Download and use our mobile applications on devices you own or control
- Access documentation and training materials provided with the Services

4.2 License Restrictions

You may NOT:

- Copy, modify, or create derivative works of the Services
- Reverse engineer, decompile, or disassemble the Services
- Rent, lease, sell, sublicense, or transfer the Services to third parties
- Remove or obscure proprietary notices or labels
- Use the Services to develop competing products or services
- Access the Services to build a similar or competitive product

- Frame or mirror any content from the Services
- Use automated tools (bots, scrapers) to access the Services (except authorized APIs)
- Exceed usage limits specified in your subscription plan

4.3 API Access

If you access our Services via APIs:

- You must comply with API documentation and usage guidelines
- Rate limits apply (as specified in your plan)
- You must not abuse or overload our infrastructure
- We may revoke API access for violations

API Terms: Separate API Terms and Conditions may apply.

4.4 Open Source Components

Our Services may include open source software components. Such components are licensed under their respective open source licenses, which are available upon request.

4.5 Mobile Applications

For mobile apps (FieldVoice):

- Downloaded from Apple App Store or Google Play Store
- Subject to respective app store terms and conditions
- Updates may be automatic or require manual installation
- May require specific device permissions (camera, location, microphone, storage)

Permissions: We will request permissions only when necessary for functionality and explain their purpose.

4.6 Offline Usage

FieldVoice offers offline functionality:

- Data stored locally on your device is encrypted
- Automatic sync when connectivity is restored
- Offline period: Up to 7 days (data must be synced within this period)
- Conflicts are resolved using "last write wins" or manual resolution

5. USER OBLIGATIONS AND PROHIBITED CONDUCT

5.1 Compliance with Laws

You agree to use the Services in compliance with all applicable laws, including but not limited to:

- **India:** Information Technology Act, 2000; DPDP Act, 2023; Clinical Establishments Act, 2010; Drugs and Cosmetics Act, 1940; Indian Penal Code, 1860
- **Healthcare Regulations:** Medical Council of India regulations; NABH standards; UCPMP
- **Pharmaceutical Regulations:** DGHS guidelines; state pharmaceutical regulations
- **Data Protection:** DPDP Act, 2023; IT Rules, 2011
- **International:** HIPAA (if applicable); GDPR (if applicable)

5.2 Acceptable Use

You agree to:

- Use the Services for lawful business purposes only
- Maintain accurate and up-to-date information
- Respect the rights and privacy of others
- Cooperate with our investigations of violations
- Promptly report bugs, security vulnerabilities, or abuse

5.3 Prohibited Conduct

You may NOT:

Illegal Activities

- Violate any applicable laws or regulations
- Infringe intellectual property rights of others
- Transmit illegal, harmful, or offensive content
- Engage in fraud, deception, or misrepresentation
- Facilitate money laundering or terrorist financing

Security Violations

- Circumvent security measures or access controls
- Probe, scan, or test vulnerabilities without authorization
- Access other users' accounts or data without permission
- Interfere with or disrupt the Services or servers
- Introduce viruses, malware, or harmful code

Data Misuse

- Collect or harvest user data without consent
- Sell, share, or misuse patient or doctor data
- Violate confidentiality obligations
- Use data for purposes not disclosed or consented to

- Transfer data in violation of data protection laws

Abuse and Harassment

- Harass, threaten, or intimidate other users
- Transmit hate speech, defamatory content, or obscene material
- Impersonate others or create fake profiles
- Engage in spam, phishing, or unsolicited marketing

Healthcare-Specific Prohibitions

- Provide medical advice or diagnosis through the Services (for non-licensed users)
- Prescribe medications or treatments through the Services
- Store or transmit patient data without proper consent
- Violate HIPAA, NABH, or other healthcare standards
- Engage in off-label promotion of pharmaceuticals (for FieldVoice users)
- Offer illegal inducements to healthcare professionals (UCPMP violations)
- Fabricate or manipulate prescription data (RCPA)

Competitive Activities

- Use the Services to develop competing products
- Benchmark performance without our written consent
- Publicly disparage our Services without factual basis
- Recruit our employees or contractors

5.4 Monitoring and Enforcement

We reserve the right to:

- Monitor use of the Services for compliance
- Investigate suspected violations
- Remove or disable access to violating content
- Suspend or terminate accounts for violations
- Cooperate with law enforcement investigations
- Report illegal activities to authorities

No Obligation: We have no obligation to monitor content or use, but may do so.

5.5 Reporting Violations

To report violations of these Terms:

- **Email:** abuse@medismo.in
- **Phone:** +91-99625-78801
- **Subject:** "Terms Violation Report - [Brief Description]"

Include:

- Your contact information
- Description of the violation
- Evidence (screenshots, links, etc.)
- Affected user or content (if known)

---

6. INTELLECTUAL PROPERTY RIGHTS

6.1 Our Intellectual Property

All intellectual property rights in the Services, including but not limited to:

- Software, source code, object code, algorithms
- User interfaces, designs, graphics, logos
- Trademarks, service marks, trade names ("Medismo," "CareConnect AI," "PatientVoice Pro," "FieldVoice")
- Content, documentation, training materials
- Patents, trade secrets, know-how
- Databases, data structures, schemas

are owned exclusively by Medismo or our licensors.

6.2 Reservation of Rights

All rights not expressly granted in these Terms are reserved by Medismo. Nothing in these Terms transfers ownership or grants licenses beyond what is explicitly stated.

6.3 Trademarks

You may not use our trademarks without prior written permission, except:

- Referencing the Services in a factual, non-commercial manner
- Including our logo in customer lists (with our approval)

6.4 Feedback and Suggestions

If you provide feedback, suggestions, or ideas about the Services:

- We may use them without compensation or attribution
- You grant us a perpetual, worldwide, royalty-free license
- You waive any rights to such feedback
- We have no obligation to implement or respond to feedback

Why: Feedback helps us improve Services for all users.

6.5 Copyright Infringement

If you believe content on our Services infringes your copyright:

DMCA Notice (for U.S. copyrights):
Email: dmca@medismo.in

Include:

- Your contact information and signature
- Identification of copyrighted work
- Location of infringing material (URL)
- Statement of good faith belief
- Statement under penalty of perjury

Indian Copyright Act Notice:
Email: copyright@medismo.in

Include:

- Proof of copyright ownership
- Details of infringing material
- Statement of infringement
- Request for removal

Response: We will investigate and remove infringing content within 72 hours if valid.

6.6 Counter-Notice

If your content was removed due to a copyright claim and you believe it was mistaken:

- Email: copyright@medismo.in
- Provide counter-notice with explanation and evidence
- We will restore content within 10-14 business days (unless claimant files legal action)

7. DATA OWNERSHIP AND USAGE RIGHTS

7.1 Your Data Ownership

"Customer Data" means all data, content, and information you upload, submit, or transmit through the Services, including:

- Doctor profiles and contact information

- Patient data (for CareConnect AI and PatientVoice Pro)
- Visit records and daily call reports (DCRs)
- Expense records and receipts
- Sample distribution data
- Feedback and communications

Ownership: You retain all ownership rights to Customer Data.

7.2 License to Us

You grant Medismo a limited, worldwide, royalty-free license to:

- Store, process, and transmit Customer Data
- Perform the Services and fulfill our obligations
- Generate analytics and insights from Customer Data
- Create anonymized, aggregated data (see Section 7.4)

Scope: This license is limited to providing the Services and terminates upon account closure (subject to retention periods).

7.3 Your Responsibilities for Customer Data

You are solely responsible for:

- Accuracy, quality, and legality of Customer Data
- Obtaining necessary consents (e.g., from patients, doctors)
- Complying with data protection laws (DPDP Act, HIPAA, etc.)
- Backing up Customer Data (we provide backups, but you should maintain independent backups)
- Security of data transmitted to our Services

We Are Not Responsible For:

- Loss or corruption of Customer Data due to your actions
- Legal violations arising from your data collection or use
- Consequences of inaccurate or incomplete data

7.4 Anonymized and Aggregated Data

We may create anonymized, aggregated data from Customer Data:

- **Anonymized:** Data that cannot be attributed to any individual
- **Aggregated:** Data combined from multiple customers (minimum 50 users)

Our Rights: We own all anonymized and aggregated data and may:

- Use it for analytics, research, and product improvement
- Share it with third parties for benchmarking or research
- Publish it in reports, case studies, or marketing materials

Your Rights: Anonymized data is NOT Personal Data under DPDP Act and is not subject to deletion requests.

Example: "Hospital readmission rates in Mumbai decreased by 25% among CareConnect AI users" (no specific hospital identified).

7.5 Data Portability

Upon request, we will provide Customer Data in machine-readable formats:

- **Formats:** CSV, JSON, XML, HL7 FHIR R4 (for healthcare data)
- **Delivery:** Secure download link or API access
- **Timeline:** Within 30 days of request
- **Fee:** First export per year is free; additional exports may incur fees

Request: Email dpo@medismo.in with subject "Data Export Request"

7.6 Data Upon Termination

Upon account termination or expiration:

- **30-Day Grace Period:** Customer Data remains accessible for download
- **After 30 Days:** Customer Data is deleted or anonymized per our retention policy (see Privacy Policy Section 10)
- **Exceptions:** Data may be retained longer if required by law or for legal claims

Download Your Data: Before terminating, export Customer Data via Account Settings → Export Data.

8. SERVICE AVAILABILITY AND MODIFICATIONS

8.1 Service Level Agreement (SLA)

Uptime Commitment

- **Target Uptime:** 99.5% per calendar month (excluding scheduled maintenance)
- **Calculation:** (Total Minutes in Month - Downtime) / Total Minutes in Month × 100
- **Scheduled Maintenance:** Up to 4 hours per month (announced 48 hours in advance)

Downtime Exclusions: Downtime caused by:

- Force majeure events (natural disasters, war, terrorism)
- Internet service provider failures
- Your equipment, software, or network issues
- Denial of service attacks or similar incidents
- Scheduled maintenance (with proper notice)

Service Credits

If we fail to meet 99.5% uptime:

- **99.0% - 99.5%:** 10% credit of monthly subscription fee
- **95.0% - 99.0%:** 25% credit
- **Below 95.0%:** 50% credit

Claiming Credits:

- Email support@medismo.in within 30 days of incident
- Include dates and details of downtime
- Credits applied to next billing cycle
- Maximum credit: 100% of monthly fee

Sole Remedy: Service credits are your sole remedy for downtime.

8.2 Scheduled Maintenance

We perform scheduled maintenance for:

- Software updates and patches
- Infrastructure upgrades
- Database optimization
- Security enhancements

Notice: 48 hours' advance notice via email and in-app notification

Timing: Typically during low-usage periods (e.g., Saturday midnight to 4 AM IST)

Duration: Up to 4 hours per month

8.3 Emergency Maintenance

For critical security issues or system failures, we may perform emergency maintenance without notice. We will:

- Post real-time status updates at status.medismo.in
- Send notifications once issue is identified
- Minimize disruption to the extent possible

8.4 Service Modifications

We may modify the Services by:

- Adding new features or functionality (may require additional fees)
- Deprecating or removing features (30 days' notice)
- Changing user interface or workflows (no notice required for minor changes)
- Updating underlying technology (no notice required)

Material Changes: For changes that significantly affect core functionality:

- 30 days' advance notice
- Explanation of changes and impact
- Option to terminate with pro-rated refund (within 30 days of notice)

8.5 Service Discontinuation

We may discontinue Services or features:

- With 90 days' advance notice for paid Services
- With 30 days' notice for free or beta Services
- Immediately for Services violating laws or posing security risks

Upon Discontinuation:

- You may download Customer Data during notice period
- Pro-rated refund for unused subscription period
- Migration assistance to alternative services (if available)

8.6 Status Page

Check real-time service status:

- **URL:** status.medismo.in
- **Updates:** Real-time incident updates, scheduled maintenance, historical uptime
- **Subscribe:** Email or SMS notifications for incidents

9. FEES, PAYMENT TERMS, AND REFUNDS

Pricing available at www.medismo.in/pricing (subject to change with 30 days' notice)

9.2 Billing Cycle

- **Monthly:** Billed on the 1st of each month
- **Annual:** Billed upfront (15% discount applied)

- **Quarterly:** Billed every 3 months (10% discount applied)

Pro-Rated: If you upgrade mid-cycle, you pay the difference immediately; if you downgrade, credit applies to next billing cycle.

9.3 Payment Methods

- **Credit/Debit Cards:** Visa, Mastercard, American Express, RuPay
- **Net Banking:** All major Indian banks
- **UPI:** Google Pay, PhonePe, Paytm
- **Bank Transfer:** Wire transfer or NEFT/RTGS (for annual plans)
- **Purchase Orders:** For enterprise customers (net 30 payment terms)

Payment Processor: Razorpay / Stripe (PCI-DSS compliant)

9.4 Automatic Renewal

Subscriptions automatically renew unless you cancel:

- **Renewal Notice:** 7 days before renewal date
- **Payment:** Charged to your payment method on file
- **Cancellation:** Cancel anytime before renewal date to avoid next charge

9.5 Taxes

All fees are exclusive of taxes. You are responsible for:

- GST (Goods and Services Tax) - 18% (India)
- Withholding taxes (if applicable)
- Any other applicable taxes or duties

GST Invoice: Provided via email within 3 business days of payment

GST Registration: Our GSTIN: [INSERT GSTIN]

9.6 Late Payment

If payment fails or is overdue:

- **Day 1-7:** Email reminder and retry payment
- **Day 8-15:** Account access restricted (read-only mode)
- **Day 16-30:** Account suspended (no access)
- **After 30 Days:** Account terminated and data deleted per retention policy

Late Fee: ₹500 or 2% of outstanding amount per month, whichever is higher

Reinstatement: Pay outstanding balance plus late fees to reactivate account.

9.7 Refund Policy

Free Trial

- No refund applicable (free of charge)

Monthly Subscriptions

- **Within 7 Days:** Full refund if you're unsatisfied
- **After 7 Days:** No refund, but you can cancel to avoid next month's charge

Annual Subscriptions

- **Within 30 Days:** Pro-rated refund for unused months (minus setup fees)
- **After 30 Days:** No refund, but you can cancel to prevent auto-renewal

Refund Exceptions (No Refund)

- Accounts terminated for Terms violations
- Downgrades or feature changes
- Unused features or functionality
- Third-party fees (payment processor, SMS, WhatsApp)

Refund Processing: 7-10 business days to original payment method

Request Refund: Email billing@medismo.in with invoice number and reason

9.8 Price Changes

We may change pricing with 30 days' advance notice:

- Existing customers: Current pricing honored until end of billing cycle
- New customers: New pricing applies immediately
- Annual plans: Price locked for entire annual period

Objection: If you do not agree with price increase, cancel before it takes effect.

9.9 Enterprise Custom Pricing

For large organizations (100+ users):

- Custom pricing based on volume, features, and support
- Negotiated contract terms
- Dedicated account manager

- Annual commitment required

Contact Sales: sales@medismo.in or +91-83349-45671

10. CONFIDENTIALITY OBLIGATIONS

10.1 Definition of Confidential Information

"Confidential Information" means any information disclosed by one party ("Disclosing Party") to the other party ("Receiving Party") that is:

- Marked as "Confidential" or similar designation
- Reasonably understood to be confidential given its nature
- Proprietary or non-public information

Examples:

- **Your Confidential Information:** Customer Data, business strategies, financial information, patient data
- **Our Confidential Information:** Software source code, algorithms, pricing, roadmaps, security measures

10.2 Obligations

The Receiving Party agrees to:

- Use Confidential Information only for purposes of this Agreement
- Protect Confidential Information with same care as its own (minimum: reasonable care)
- Not disclose Confidential Information to third parties (except as permitted)
- Limit access to employees and contractors on a need-to-know basis
- Ensure employees/contractors are bound by confidentiality obligations

10.3 Exceptions

Confidential Information does NOT include information that:

- Is or becomes publicly available (through no breach by Receiving Party)
- Was rightfully known to Receiving Party before disclosure
- Is independently developed by Receiving Party without use of Confidential Information
- Is rightfully received from a third party without confidentiality obligations

10.4 Required Disclosures

Receiving Party may disclose Confidential Information if required by:

- Court order, subpoena, or legal process
- Regulatory authorities (e.g., Medical Council investigations)
- Law enforcement

Procedure: Receiving Party will:

- Notify Disclosing Party promptly (unless legally prohibited)
- Cooperate in seeking protective order
- Disclose only minimum necessary information

10.5 Term

Confidentiality obligations survive for:

- **Customer Data:** Duration of Agreement + 3 years
- **Trade Secrets:** Indefinitely (or until no longer a trade secret)
- **Other Confidential Information:** 5 years after disclosure

10.6 Return or Destruction

Upon termination or request, Receiving Party will:

- Return or destroy all Confidential Information
- Provide written certification of destruction (if requested)
- Exception: May retain copies required by law or for backup (subject to continued confidentiality)

11. INDEMNIFICATION

11.1 Your Indemnification

You agree to indemnify, defend, and hold harmless Medismo, its affiliates, officers, directors, employees, agents, and licensors from and against any claims, liabilities, damages, losses, costs, and expenses (including reasonable attorneys' fees) arising out of or related to:

- Your use or misuse of the Services
- Your violation of these Terms
- Your violation of any law or regulation
- Your violation of third-party rights (including intellectual property, privacy, or data protection rights)
- Customer Data you provide or transmit
- Your negligence or willful misconduct

Examples:

- Doctor files complaint that you collected their data without consent → You indemnify us
- Patient sues for privacy violation due to your data handling → You indemnify us
- Competitor sues for intellectual property infringement based on your content → You indemnify us

11.2 Our Indemnification

We agree to indemnify, defend, and hold you harmless from claims that:

- The Services infringe third-party intellectual property rights (patents, copyrights, trademarks)

Conditions:

- You promptly notify us of the claim in writing
- You give us sole control of defense and settlement
- You cooperate reasonably in the defense

Remedies: If Services are found to infringe, we may (at our option):

- Obtain a license for you to continue using the Services
- Replace or modify the Services to be non-infringing
- Terminate the Services and refund prepaid, unused fees

11.3 Exclusions from Our Indemnification

We will NOT indemnify for claims arising from:

- Your modification of the Services
- Your combination of Services with third-party products
- Your use of Services in violation of these Terms
- Customer Data or content you provide
- Your compliance or non-compliance with laws

11.4 Procedure

Indemnification Process:

1. Indemnified party promptly notifies indemnifying party of claim
2. Indemnifying party assumes control of defense (with competent counsel)
3. Indemnified party cooperates reasonably and may participate at own expense
4. Indemnifying party may not settle without indemnified party's consent (not to be unreasonably withheld)

12. LIMITATION OF LIABILITY

12.1 Disclaimer of Consequential Damages

TO THE MAXIMUM EXTENT PERMITTED BY LAW, MEDISMO SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING:

- Loss of profits, revenue, or business opportunities
- Loss of data or use of Services
- Business interruption or downtime
- Reputational harm or loss of goodwill
- Cost of substitute goods or services

EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12.2 Cap on Liability

OUR TOTAL AGGREGATE LIABILITY FOR ALL CLAIMS ARISING OUT OF OR RELATED TO THESE TERMS OR THE SERVICES SHALL NOT EXCEED THE GREATER OF, WHICHEVER IS LOWER:

- **₹1,00,000 (One Lakh Rupees), OR**
- **TOTAL FEES PAID BY YOU IN THE 12 MONTHS PRECEDING THE CLAIM**

12.3 Exceptions

The limitations in Sections 12.1 and 12.2 do NOT apply to:

- Your indemnification obligations (Section 11)
- Your payment obligations (Section 9)
- Our indemnification obligations (Section 11.2)
- Liability for gross negligence or willful misconduct
- Liability for death or personal injury caused by negligence
- Liability that cannot be excluded under Indian law

12.4 Allocation of Risk

The limitations of liability reflect an allocation of risk between the parties. The fees you pay reflect this allocation and limitation. Without these limitations, the fees would be substantially higher.

12.5 Acknowledgment

You acknowledge and agree that:

- We are not liable for actions or inactions of third parties (e.g., payment processors, cloud providers)
- We are not liable for unauthorized access resulting from your failure to secure credentials
- We are not liable for loss of data if you fail to maintain backups
- We are not liable for delays or failures due to force majeure events

13. WARRANTIES AND DISCLAIMERS

13.1 Limited Warranty

We warrant that the Services will perform materially in accordance with our documentation under normal use. This warranty:

- Lasts for 30 days from first use
- Is void if you breach these Terms
- Does not cover issues caused by your misuse, modifications, or third-party products

Remedy: If we breach this warranty, we will use commercially reasonable efforts to correct the issue. If unable to correct within 30 days, you may terminate and receive a pro-rated refund.

13.2 Disclaimer of Other Warranties

EXCEPT FOR THE LIMITED WARRANTY ABOVE, THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTIES OF ANY KIND.

WE DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO:

- **Merchantability:** Services fit for ordinary purposes
- **Fitness for a Particular Purpose:** Services meet your specific needs
- **Non-Infringement:** Services do not violate third-party rights
- **Title:** Ownership rights
- **Accuracy or Reliability:** Results or outputs from Services
- **Uninterrupted or Error-Free Operation:** Services will be available 100% of the time

13.3 Healthcare-Specific Disclaimers

Not a Medical Device (CareConnect AI, PatientVoice Pro)

- Services are decision-support tools, NOT medical devices
- NOT intended to diagnose, treat, cure, or prevent any disease
- NOT a substitute for professional medical judgment
- Risk scores and predictions are estimates, not diagnoses

- Healthcare providers must independently verify all information

Regulatory Status: Our Services are NOT approved or cleared by FDA (USA), CDSCO (India), or other medical device regulators.

Not Medical Advice

- We do not provide medical advice, diagnosis, or treatment
- No doctor-patient relationship is created
- Always consult qualified healthcare professionals for medical decisions

Clinical Validation

- AI algorithms are validated on historical data but may not generalize to all populations
- Performance metrics (e.g., accuracy, sensitivity) are estimates based on test data
- Real-world performance may vary

13.4 Third-Party Services

We disclaim all warranties for:

- Third-party integrations (HIS/EMR systems, payment gateways, communication platforms)
- Third-party content (medical databases, research papers)
- Internet connectivity and infrastructure

Your Responsibility: You are responsible for evaluating and accepting risks associated with third-party services.

13.5 Data Accuracy

We do not warrant that:

- Customer Data will be accurate or complete
- Data entered by users will be error-free
- Analytics or reports will be accurate (dependent on data quality)

Your Responsibility: You are responsible for reviewing and verifying all data and outputs.

13.6 Security

While we implement robust security measures (Section 9 of Privacy Policy), we do not warrant that:

- Services will be completely secure or free from vulnerabilities
- Unauthorized access will never occur

- Data breaches will never happen

Why: No system is 100% secure. We commit to industry-standard security, not absolute security.

14. TERMINATION AND SUSPENSION

14.1 Termination by You

You may terminate your account at any time:

- **Self-Service:** Account Settings → Cancel Subscription
- **Email:** support@medismo.in
- **Effective Date:** End of current billing cycle (no mid-cycle refunds for monthly plans)

Effect of Termination:

- Access to Services immediately ends (after billing cycle)
- Customer Data remains accessible for 30 days for download
- After 30 days, Customer Data is deleted per our retention policy
- No refund for unused portion of subscription (except as stated in Section 9.7)

14.2 Termination by Us

For Cause

We may terminate or suspend your account immediately if:

- You breach any material term of this Agreement
- You fail to pay fees when due (after 30-day grace period)
- You engage in prohibited conduct (Section 5.3)
- You violate laws or regulations
- Your use poses security or legal risk to us or others
- You provide false or misleading information

Notice: We will notify you via email of termination and reasons (unless legally prohibited or security risk)

No Refund: No refund will be provided for terminations for cause

For Convenience

We may terminate free accounts or beta access at any time with 30 days' notice, without cause.

Paid Accounts: We will not terminate paid accounts for convenience except upon 90 days' notice with pro-rated refund.

14.3 Suspension

Temporary Suspension

We may suspend (without terminating) your account if:

- Your account is under investigation for Terms violation
- Your account poses an immediate security threat
- Your use threatens system stability or other users
- Payment is overdue (15+ days)
- We receive court order or regulatory directive

Duration: Suspension lasts until issue is resolved or account is terminated

Access During Suspension: Read-only access may be provided to retrieve data

Reinstatement: Resolve the issue (e.g., pay overdue fees, address security concerns) to reinstate

Notice

We will provide notice of suspension and reasons, except:

- When immediate suspension is necessary for security
- When notice is legally prohibited
- When account is engaged in ongoing abuse

14.4 Effect of Termination

Immediate Effects

- All licenses granted under these Terms terminate
- Your access to Services immediately ends (except 30-day data retrieval period)
- Outstanding fees become immediately due and payable
- You must cease all use of our trademarks and branding

Data Retention

- **30-Day Grace Period:** Customer Data remains accessible for download
- **After 30 Days:** Data is deleted per our retention policy (Privacy Policy Section 10)
- **Legal Holds:** Data subject to legal obligations may be retained longer

Surviving Provisions

The following sections survive termination:

- Payment obligations (Section 9)
- Intellectual Property (Section 6)
- Confidentiality (Section 10)
- Indemnification (Section 11)
- Limitation of Liability (Section 12)
- Dispute Resolution (Section 16)
- Governing Law (Section 17)

14.5 Reactivation

Terminated accounts may be reactivated at our discretion:

- Contact support@medismo.in
- Resolve issues that led to termination
- Pay any outstanding fees
- Agree to comply with Terms going forward

No Guarantee: We reserve the right to refuse reactivation.

15. DISPUTE RESOLUTION AND ARBITRATION

15.1 Informal Resolution

Before initiating formal dispute resolution, the parties agree to negotiate in good faith for at least 30 days:

- **Notice:** Send written notice describing the dispute to legal@medismo.in
- **Meeting:** Parties will meet (in person or virtually) to discuss resolution
- **Timeline:** 30 days from notice to attempt resolution

Exception: Either party may seek injunctive relief without informal negotiation if necessary to prevent irreparable harm.

15.2 Mediation

If informal resolution fails, parties agree to mediation:

- **Mediator:** Mutually agreed neutral mediator
- **Location:** Kolkata, West Bengal, India
- **Cost:** Split equally between parties
- **Confidential:** All mediation communications are confidential
- **Non-Binding:** Mediation is non-binding unless settlement reached

15.3 Arbitration

If mediation fails, all disputes shall be resolved by binding arbitration:

Arbitration Rules

- **Administered By:** Kolkata International Arbitration
- **Rules:** MCIA Arbitration Rules (current version)
- **Alternative:** Indian Council of Arbitration (ICA) if MCIA unavailable

Arbitrator

- **Number:** One (1) arbitrator for disputes under ₹50 lakhs; three (3) arbitrators for larger disputes
- **Qualifications:** Experience in technology and healthcare law
- **Appointment:** Mutually agreed within 30 days; otherwise appointed by MCIA

Seat and Language

- **Seat of Arbitration:** Kolkata, West Bengal, India
- **Language:** English

Procedure

- **Discovery:** Limited discovery as determined by arbitrator
- **Hearing:** In-person or virtual hearing
- **Timeline:** Award within 6 months of arbitrator appointment (extendable by arbitrator)
- **Confidentiality:** All arbitration proceedings are confidential

Award

- **Final and Binding:** Arbitration award is final and binding on both parties
- **Enforcement:** Award may be entered as judgment in any court of competent jurisdiction
- **Limited Appeal:** No appeal except as permitted under Indian Arbitration and Conciliation Act, 1996

Cost Allocation

- **ICA Fees:** As per ICA fee schedule
- **Arbitrator Fees:** As determined by ICA
- **Allocation:** Each party bears its own legal fees; arbitrator determines allocation of arbitration costs in award

15.4 Class Action Waiver

YOU AGREE THAT DISPUTES WILL BE RESOLVED ONLY ON AN INDIVIDUAL BASIS AND NOT AS A CLASS ACTION, CONSOLIDATED ACTION, OR REPRESENTATIVE ACTION.

You waive any right to:

- Participate in class action lawsuits
- Serve as class representative
- Consolidate your dispute with others

Why: This enables efficient, cost-effective dispute resolution.

Severability: If class action waiver is found unenforceable, the arbitration agreement does not apply to that dispute (it proceeds in court).

15.5 Small Claims Court

Notwithstanding the arbitration agreement, either party may bring an individual action in small claims court if:

- The dispute qualifies for small claims court jurisdiction
- The dispute remains in small claims court (not removed or appealed to higher court)

15.6 Injunctive Relief

Either party may seek temporary or preliminary injunctive relief in any court of competent jurisdiction to:

- Protect intellectual property rights
- Prevent data breaches or security incidents
- Enforce confidentiality obligations
- Prevent irreparable harm

Arbitration Continues: Seeking injunctive relief does not waive right to arbitrate other aspects of dispute.

15.7 Opt-Out

You may opt out of the arbitration agreement:

- **Timeline:** Within 30 days of first accepting these Terms
- **Method:** Email legal@medismo.in with subject "Arbitration Opt-Out"
- **Include:** Your name, email, organization, and statement "I opt out of arbitration"
- **Effect:** Disputes will be resolved in courts per Section 17.2

Cannot Opt Out Later: Once 30-day period passes, you cannot opt out.

16. GOVERNING LAW AND JURISDICTION

16.1 Governing Law

These Terms and any disputes arising out of or related to these Terms or the Services shall be governed by and construed in accordance with the laws of India, specifically:

- **Indian Contract Act, 1872**
- **Information Technology Act, 2000**
- **Digital Personal Data Protection Act, 2023**
- **Arbitration and Conciliation Act, 1996**

Exclusion: The UN Convention on Contracts for the International Sale of Goods does not apply.

16.2 Exclusive Jurisdiction (If Not Arbitrating)

If you opt out of arbitration (Section 15.7), the courts of Kolkata, West Bengal, India shall have exclusive jurisdiction over any disputes.

16.3 Language

These Terms are drafted in English. If translated into other languages, the English version controls in case of conflict.

16.4 Waiver of Jury Trial (If Applicable)

To the extent permitted by law, both parties waive any right to trial by jury.

17. COMPLIANCE WITH HEALTHCARE REGULATIONS

17.1 Clinical Establishments Act Compliance

Healthcare providers using CareConnect AI and PatientVoice Pro must:

- Hold valid registration under Clinical Establishments (Registration and Regulation) Act, 2010 (or equivalent state law)
- Maintain all required licenses and permits
- Comply with quality and safety standards
- Not use Services to circumvent regulatory requirements

17.2 NABH Accreditation

If you are NABH-accredited:

- You are responsible for ensuring use of Services complies with NABH standards
- We provide tools and reports to support compliance, but do not guarantee NABH compliance
- You must maintain all required documentation and records

17.3 Medical Council Regulations

Healthcare professionals using Services must:

- Hold valid registration with Medical Council of India or State Medical Council
- Comply with Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
- Not engage in unethical practices through Services (e.g., fee splitting, commission-based referrals)
- Maintain patient confidentiality per Section 1.3 of MCI Regulations

17.4 Pharmaceutical Regulations (FieldVoice)

DGHS Guidelines

Medical representatives and pharmaceutical companies must:

- Comply with Department of Health and Family Services (DGHS) guidelines for pharmaceutical marketing
- Maintain accurate records of interactions with healthcare professionals
- Not engage in off-label promotion of drugs

UCPMP (Uniform Code of Pharmaceutical Marketing Practices)

You agree to comply with UCPMP, including:

- **Gifts and Hospitality:** Not exceed limits specified in UCPMP (currently ₹1,000 per event)
- **Transparency:** Disclose all gifts, hospitality, and sponsorships
- **No Inducements:** Not offer inducements to prescribe specific drugs
- **Accurate Information:** Provide truthful, balanced, and evidence-based information
- **Adverse Event Reporting:** Report adverse events through appropriate channels

FieldVoice Compliance Tools:

- Gift limit tracking and alerts
- UCPMP-compliant visit templates
- Automated compliance reports for internal audits

Drugs and Cosmetics Act

You must comply with:

- Drugs and Cosmetics Act, 1940
- Drugs and Cosmetics Rules, 1945
- Sample distribution regulations
- Labeling and packaging requirements

Sample Management: FieldVoice tracks sample distribution with:

- Batch and expiry date tracking
- Doctor acknowledgment capture
- Audit trails for regulatory inspections

17.5 HIPAA (If Applicable)

If you are a U.S. healthcare provider subject to HIPAA:

- A separate Business Associate Agreement (BAA) is required
- Contact legal@medismo.in to execute BAA before processing Protected Health Information (PHI)
- Without a BAA, do NOT enter PHI into the Services
- Additional HIPAA-specific terms apply (Appendix B)

17.6 GDPR (If Applicable)

If you are in the European Economic Area (EEA) or process data of EEA residents:

- Additional GDPR-specific terms apply (Appendix A)
- EU Standard Contractual Clauses are incorporated by reference
- We act as Data Processor; you are Data Controller

17.7 Your Regulatory Obligations

You acknowledge that:

- You are solely responsible for complying with all applicable healthcare regulations
- We provide tools to support compliance but do not guarantee compliance
- You must independently verify that your use of Services complies with your regulatory obligations
- We are not liable for your regulatory violations or penalties

Compliance Support: We offer:

- Documentation and reports for regulatory audits
- Consultation with compliance experts (additional fees may apply)
- Customization to meet specific regulatory requirements (Enterprise plans)

18. FORCE MAJEURE

18.1 Definition

"**Force Majeure Event**" means any event beyond our reasonable control, including but not limited to:

- Natural disasters (earthquakes, floods, hurricanes, tsunamis)
- Pandemics, epidemics, or public health emergencies
- War, terrorism, riots, civil unrest, or acts of government
- Strikes, labor disputes, or lockouts (not involving our employees)
- Failure of public utilities, telecommunications, or Internet infrastructure
- Cyber attacks, DDoS attacks, or malicious hacking (despite reasonable security measures)
- Fire, explosion, or other catastrophic events
- Acts of God

18.2 Effect on Obligations

During a Force Majeure Event:

- We are excused from performing obligations to the extent prevented by the event
- Obligations are suspended (not terminated) for the duration of the event
- We will use commercially reasonable efforts to resume performance
- SLA commitments (Section 8.1) and uptime guarantees do not apply

18.3 Notice and Updates

We will:

- Notify you promptly upon becoming aware of a Force Majeure Event
- Provide regular updates on status and expected duration
- Notify you when the event ends and services are restored

18.4 Termination

If a Force Majeure Event lasts longer than 60 consecutive days:

- Either party may terminate this Agreement upon written notice
- You will receive a pro-rated refund for unused subscription period
- No other liability for termination due to Force Majeure

18.5 Mitigation

We will:

- Take reasonable steps to mitigate impact of Force Majeure Events
- Implement disaster recovery and business continuity plans
- Restore services as quickly as reasonably possible

19. ENTIRE AGREEMENT AND SEVERABILITY

19.1 Entire Agreement

These Terms, together with:

- Privacy Policy
- Service Level Agreement (SLA)
- Data Processing Agreement (if applicable)
- Business Associate Agreement (if applicable)
- Any Order Forms or Statements of Work

constitute the entire agreement between you and Medismo regarding the Services and supersede all prior agreements, understandings, and communications (oral or written).

19.2 Amendments

These Terms may only be amended by:

- A written agreement signed by both parties (for custom enterprise agreements)
- Updated Terms posted on our website (for standard subscriptions, per Section 15)

No Other Amendments: Oral agreements, purchase orders, or other documents do not modify these Terms unless explicitly incorporated.

19.3 Severability

If any provision of these Terms is found by a court of competent jurisdiction to be invalid, illegal, or unenforceable:

- The invalid provision will be modified to the minimum extent necessary to make it enforceable
- If modification is not possible, the invalid provision will be severed
- All other provisions remain in full force and effect

19.4 Interpretation

In case of ambiguity or conflict:

- Specific provisions prevail over general provisions
- Examples are illustrative and not limiting
- Headings are for convenience only and do not affect interpretation
- "Including" means "including without limitation"
- Singular includes plural and vice versa

19.5 Order of Precedence (For Conflicts)

In the event of conflict between documents, the order of precedence is:

1. Executed Order Form or Statement of Work (if any)
2. Business Associate Agreement or Data Processing Agreement (if applicable)
3. These Terms of Service
4. Privacy Policy
5. Service Level Agreement

20. ASSIGNMENT AND TRANSFER

20.1 Your Assignment

You may NOT assign or transfer your rights or obligations under these Terms without our prior written consent, including:

- Merger, acquisition, or change of control
- Asset sale or divestiture
- Sublicensing to third parties

Exception: Assignment to a successor entity as part of reorganization (provided successor assumes all obligations) may be permitted with 30 days' notice.

Effect of Unauthorized Assignment: Any attempted assignment without consent is void.

20.2 Our Assignment

We may freely assign or transfer our rights and obligations under these Terms, including:

- To an affiliate or subsidiary
- In connection with merger, acquisition, reorganization, or sale of assets
- To a successor entity

Notice: We will notify you of any assignment that materially affects your rights.

20.3 Effect of Assignment

Upon valid assignment:

- Assignee assumes all rights and obligations
- You agree to cooperate with assignee
- Prior assignor is released from obligations (unless otherwise agreed)

ADDITIONAL PROVISIONS

21. Relationship of Parties

Nothing in these Terms creates a partnership, joint venture, agency, or employment relationship between you and Medismo. You are an independent contractor.

22. No Third-Party Beneficiaries

These Terms are for the benefit of you and Medismo only. No third party has any right to enforce any provision of these Terms.

Exception: Our affiliates, directors, officers, employees, and agents are third-party beneficiaries of limitation of liability and indemnification provisions.

23. Waiver

Failure or delay by either party to enforce any provision does not constitute a waiver of that provision or any other provision. Waiver must be in writing and signed by the waiving party.

24. Notices

To You

We may provide notices to you by:

- Email to your registered email address
- In-app notifications
- Posting on our website
- Physical mail to your registered address (for legal notices)

Deemed Received:

- Email: 24 hours after sending
- In-app: When displayed
- Mail: 5 business days after sending

To Us

You may provide notices to us by:

- **General Inquiries:** support@medismo.in
- **Legal Notices:** legal@medismo.in
- **Physical Mail:**
  Medismo LifeTech(Allied BizTech Solutions Private Limited)
  Registered Address: 1ST FLOOR, NO.4, WELDER STREET, ANNA SALAI, Chennai, Tamil Nadu, 600002

  Mailing Address: Medismo LifeTech (Allied BizTech Solutions pvt. Ltd.) off Biswa Bangla Sarani, Chinar Park, Noapara, Sukanta Pally, Newtown, Kolkata, West Bengal 700157

Required for Legal Notices: Physical mail with signature confirmation

25. Export Compliance

You agree to comply with all applicable export control laws, including:

- Export Control Laws of India
- U.S. Export Administration Regulations (if applicable)
- EU Export Controls (if applicable)

You represent that you are not:

- Located in a country subject to U.S. or Indian government embargo
- Listed on any government list of prohibited or restricted parties

26. Government Use

If you are a government entity or contractor:

- Our Services are "commercial items" as defined under FAR 2.101 (if applicable)
- Use, reproduction, and disclosure are subject to these Terms
- No additional rights or warranties apply

27. Language

These Terms are drafted in English. Any translation is for convenience only. In case of conflict, the English version prevails.

28. Survival

Provisions that by their nature should survive termination will survive, including but not limited to:

- Payment obligations
- Intellectual property rights
- Confidentiality

- Indemnification
- Limitation of liability
- Dispute resolution
- Governing law

CONTACT INFORMATION

For Questions About These Terms:
Email: legal@medismo.in
Phone: +91-83349-45671

For Technical Support:
Email: support@medismo.in
Phone: +91-83349-45671
Hours: Monday-Friday, 9 AM - 6 PM IST

For Billing Questions:
Email: billing@medismo.in
Phone: +91-83349-45671

For Sales Inquiries:
Email: sales@medismo.in
Phone: +91-83349-45671

ACKNOWLEDGMENT

BY CLICKING "I AGREE," "ACCEPT," OR SIMILAR BUTTON, OR BY ACCESSING OR USING THE SERVICES, YOU ACKNOWLEDGE THAT:

1. You have read and understood these Terms of Service
2. You agree to be bound by these Terms
3. You have read and understood our Privacy Policy
4. You have the authority to enter into this Agreement
5. You are at least 18 years old
6. You will comply with all applicable laws and regulations

Last Updated: October 22, 2025
Effective Date: November 1, 2025
Version: 1.0

APPENDIX A: GDPR-SPECIFIC PROVISIONS

(Applicable if you are in the EEA or process data of EEA residents)

[This section would include detailed GDPR-specific provisions including EU Standard Contractual Clauses, data subject rights, data transfers, etc. - approximately 10-15 pages]

Key GDPR Rights:

- Right to access, rectify, erase, restrict processing, data portability
- Right to object to processing
- Right to lodge complaint with supervisory authority
- Right to withdraw consent

EU Representative (if required):
Available on request, project basis

APPENDIX B: HIPAA-SPECIFIC PROVISIONS

(Applicable if you are a U.S. healthcare provider subject to HIPAA)

Business Associate Agreement (BAA) Required

This appendix applies only if:

- You are a Covered Entity under HIPAA
- A separate BAA has been executed between parties

Key HIPAA Obligations:

- We act as Business Associate; you are Covered Entity
- We will use and disclose PHI only as permitted by BAA
- We implement administrative, physical, and technical safeguards
- We report breaches affecting 500+ individuals to HHS
- We allow access to PHI by individuals and HHS
- We return or destroy PHI upon termination (if feasible)

To Execute BAA:
Email: hipaa@medismo.in
Subject: "Business Associate Agreement Request"

END OF TERMS OF SERVICE

Medismo LifeTech(Allied BizTech Solutions Private Limited)
Version: 1.0