~~V0.112924,~~ ~~v1.102225~~, v1.121125

ChatRx & ChatMD

Notice of Privacy Policy and Consumer Data Consent

[First name] [Last Name]

This Notice explains how ChatRx Telemedicine and the ChatMD medical device collect, use, share, and protect your information under federal and state privacy laws. By using ChatRx or ChatMD services, you consent to the data practices described in this Notice.

This Privacy Policy complies with:

- HIPAA Privacy, Security, and Breach Notification Rules (45 CFR §§160, 164)
- FTC Health Breach Notification Rule (16 CFR Part 318)
- CCPA/CPRA (California Consumer Privacy Act as amended by CPRA 2023)
- Colorado Privacy Act (CPA)
- Virginia Consumer Data Protection Act (VCDPA)
- Connecticut Data Privacy Act (CTDPA)
- Utah Consumer Privacy Act (UCPA)
- Applicable state telehealth privacy and identity-verification laws
- FDA SaMD expectations related to data transparency and AI disclosures

~~V0.112924,~~ ~~v1.102225~~, v1.121125

1. Types of Information We Collect

ChatRx collects two categories of data:

A. Protected Health Information (PHI)

Regulated by HIPAA. Examples include:

- Symptoms provided through the ChatMD structured messaging system
- Medical history and medication lists
- Diagnoses, prescriptions, encounter notes, clinical recommendations

B. Personal Information (PI)

Regulated by CCPA/CPRA and state consumer privacy laws. Examples include:

- Name, address, email, phone
- IP address, device identifiers, geolocation data
- Cookie identifiers and usage analytics
- Payment tokens (via Stripe/PayPal, never full card numbers)
- Identity verification results from Persona

Category	Examples	Legal Basis for Processing
Personal Identifiers	Name, DOB, address, email, phone, IP address, device ID	Legitimate interest + user consent
Health Information (PHI)	Symptoms, medical history, prescriptions, clinical messages	HIPAA Treatment, Payment, Operations
Payment Information	Stripe tokenized payment data	Contractual necessity
Technical Data	Cookies, usage logs, geolocation	Consent / Opt-out rights (under CCPA)

2. How We Use Your Information

We use your information only for the following purposes:

~~V0.112924,~~ ~~v1.102225~~, v1.121125

A. HIPAA Treatment, Payment, and Operations

- Provide telemedicine services
- Issue prescriptions
- Coordinate care with pharmacies
- Verify payment and eligibility
- Perform quality improvement and compliance monitoring
- Operate the ChatMD medical device and clinical workflows

B. Legal and Regulatory Requirements

- HIPAA compliance
- FTC breach notification duties
- FDA medical device reporting (non-identifiable unless required by law)
- State telehealth and identity verification laws

C. AI-Assisted Functionality (Transparency Requirement)

ChatMD uses AI to guide structured symptom collection.
AI does **not** diagnose, determine medical advice, or make treatment decisions.
Licensed clinicians make all clinical decisions.

D. Optional De-Identified Research / AI Optimization

Used **only with explicit opt-in consent** and never with identifiable PHI.

E. No Selling of Personal or Health Information

ChatRx **does not sell** PHI or PI under any circumstances.

3. Disclosures to Third Parties

We share information only with authorized vendors operating under HIPAA Business Associate Agreements (BAAs) or state-required Data Processing Agreements (DPAs).
Your vendor table is preserved and compliant.

Examples of Authorized Vendors:

- AWS (cloud hosting, encryption)
- DoseSpot/Surescripts (e-prescribing)
- Persona (identity verification)
- Greenlight Guru (QMS and CAPA tracking)
- SmartData Inc. (software development & QA support)
- Stripe/PayPal (payment processing)
- GoHighLevel (email and SMS where permitted)
- Compliancy Group (HIPAA and privacy audits)

We do **not** disclose information to advertisers, data brokers, or social media platforms.

4. Data Retention and Deletion

Data Retention and Deletion

Data Type	Retention Period	Deletion Method
Clinical Records (PHI)	7 years (minimum HIPAA standard)	Encrypted deletion via AWS S3 Lifecycle
Consumer Accounts	3 years post inactivity	Secure purge after identity verification
Audit Logs	10 years	Immutable archive (CloudTrail / Glacier)
Marketing Data	24 months	Automated Mailchimp workflow
AI Training Data (de-identified)	Indefinite aggregate use	Stored in non-PHI RAG DB

- PHI cannot be deleted prior to mandatory federal or state retention periods.
- Deletion of PI requires identity verification through Persona + OTP.
- Audit logs are maintained for legal and security purposes.
- De-identified AI training data is stored separately in a non-PHI RAG database.

~~V0.112924, v1.102225~~, v1.121125

5. Security Measures

- AES-256 encryption at rest (AWS KMS)
- TLS 1.3 encryption in transit
- Role-based access controls (IAM least privilege)
- MFA for all administrative accounts
- Quarterly risk assessments (Compliancy Group)
- Continuous monitoring (AWS GuardDuty & Security Hub)

• Zero-trust administrative access controls
• Continuous vulnerability scanning
• Annual penetration testing
• SOC 2–aligned operational controls (non-certified but aligned)

6. Cookies and Analytics (Required by CCPA/CPRA)

ChatRx uses cookies only for:

• Authentication
• Security and session integrity
• Load balancing
• Anonymized analytics to improve system performance

We do **not** use cookies for advertising, cross-site tracking, or targeted marketing.

Users may opt out of non-essential cookies through browser settings or the Privacy Dashboard.

7. Children's and Minor Privacy

Per CCPA, COPPA, and state minor-consent laws:

• ChatRx does not knowingly collect personal data from children under age 13 without verifiable parental consent (COPPA).
• For ages 13–17, affirmative opt-in is required before sharing or processing sensitive

information.
• For minors seeking telemedicine services, eligibility follows ChatRx's Minor Consent and Emancipation Policy.

8. Consumer Privacy Rights (State Laws)

A. Under CCPA/CPRA (California + Similar States)

Users have the right to:

1. Know what information is collected and why
2. Access personal information
3. Correct inaccurate information
4. Delete personal information (with HIPAA exceptions)
5. Opt-out of sale or sharing (ChatRx does not sell data)
6. Limit use of sensitive information
7. Avoid discrimination for exercising privacy rights

B. Under Colorado, Virginia, Connecticut, and Utah Laws

Users may also:

• Opt out of profiling and targeted advertising (ChatRx does not perform these activities)
• Request data portability
• Exercise privacy rights through authenticated requests

Requests must be verified through Persona + OTP as specified in the original file.

9. How to Exercise Privacy Rights

• Submit request via Privacy Dashboard or email privacy@chatrx.md

• Identity verification required
• Acknowledgment within 10 days
• Response within legally required timelines (30–45 days depending on jurisdiction)

10. Breach Notification Practices

If unsecured data is accessed without authorization, we will notify:

- Affected individuals and the FTC within 60 days per FTC Rule
- HHS OCR if PHI is involved (HIPAA §164.404)
- State regulators if required

Notification includes incident details, data types involved, and remediation steps. (See 6.2.3 FTC Breach Notification SOP)

• Notifications occur without unreasonable delay and no later than required by law
• Breach notices include:
– Description of the incident
– Types of information involved
– Steps taken by ChatRx
– Recommendations for patient protection
• FTC notification required for unauthorized disclosure of non-HIPAA health data
• Multistate breach rules apply where more stringent than federal standards

11. Your Responsibilities as a User

You are responsible for:

• Providing accurate and complete information
• Keeping your login credentials secure
• Updating your information when it changes
• Reviewing updates to this Notice periodically

12. Updates to This Notice

ChatRx may revise this Notice as laws evolve.
Updates will be posted in the ChatRx Trust Center, and material changes will require new user acknowledgment at login.

~~V0.112924, v1.102225~~, v1.121125

13. Contact Information

ChatRx / ChatMD Compliance Division
328 S. Michigan St., Plymouth, IN 46563
privacy@chatrx.md(574) 933-2634