

At **ChatRx** and **ChatMD**, we are committed to protecting your personal and health information with industry-leading data security standards. Our **Data Security Policy** outlines the measures we take to safeguard user data, ensure compliance with HIPAA and FDA regulations, and protect against unauthorized access.

1. Data Security & HIPAA Compliance

ChatRx follows the **Health Insurance Portability and Accountability Act (HIPAA)** to ensure the confidentiality, integrity, and security of all protected health information (PHI). This includes:

- ✔ **Encryption:** All PHI and sensitive user data are encrypted **both in transit and at rest** using industry-standard AES-256 encryption protocols.
- ✔ **Access Control:** Only authorized personnel have access to user data, and all access is logged and monitored for security purposes.
- ✔ **Secure Storage:** Data is stored in **HIPAA-compliant cloud servers** with **multi-factor authentication (MFA)** and role-based access controls.
- ✔ **Data Transmission:** All communications between users, providers, and our platform use **end-to-end encryption (TLS 1.2 or higher)**.
- ✔ **Audit Trails:** All user interactions, transactions, and access logs are monitored to ensure data integrity and compliance.

📌 **For more information on our HIPAA practices, visit our [Privacy Policy](#).**

2. FDA Compliance & Data Safeguards for ChatMD

As an **FDA Class 1 medical device**, **ChatMD** is required to follow regulatory controls to ensure safe and effective use. Our data security measures for ChatMD include:

- ◆ **Device Data Integrity:** ChatMD does not store or retain PHI within the device itself; all data is securely transferred to HIPAA-compliant storage.
- ◆ **Secure Software Updates:** All software updates and patches are tested and validated to comply with FDA general controls.
- ◆ **System Monitoring:** ChatMD undergoes continuous **cybersecurity risk assessments** to mitigate vulnerabilities.
- ◆ **User Authentication:** ChatMD requires **secure user authentication** to prevent unauthorized access to the symptom assessment tool.

2-19-25

 For more information on ChatMD's FDA compliance, visit our [Regulatory Compliance Page](#).

3. FTC Compliance & Consumer Data Protection

ChatRx adheres to **Federal Trade Commission (FTC) guidelines** for **data protection and consumer transparency**. This includes:

- ◆ **No Unauthorized Data Sharing:** We do not sell, rent, or share user data with third parties for marketing purposes.
- ◆ **User Control:** Users can request access, modification, or deletion of their data in accordance with applicable laws.
- ◆ **Cookie & Tracking Transparency:** Our website notifies users about cookies, tracking technologies, and their data rights.

 For details on how we use and protect consumer data, visit our [Privacy Policy](#).

4. Data Retention & User Rights

We retain user data only as long as necessary for compliance with **legal, medical, and operational requirements**.


Retention Periods:

- Medical records: **Retained per state and federal guidelines for healthcare providers.**
- Account Information: **Deleted upon user request, except where legally required to be retained.**
- Non-PHI Usage Data: **Used for analytics and deleted after a specified period per our internal policies.**

◆ **Your Rights:** Users can request:




- ✓ A copy of their stored data
- ✓ Correction of inaccurate information
- ✓ Deletion of their account and data, subject to regulatory retention requirements

2-19-25

 To submit a data request, contact us at trust@chatrx.md

5. Complaint Handling & Security Incident Reporting

We take all data security concerns seriously. Users can report:

-  **Data breaches or suspected unauthorized access**
-  **Concerns about data security or privacy**
-  **Any suspicious activity related to their ChatRx account**

 **Reporting Process:**




 **Submit security concerns via email at trust@chatrx.md**

If a **data breach occurs**, affected users will be notified **as required by HIPAA and state laws**.

 **For regulatory or legal inquiries, contact our compliance team at trust@chatrx.md**

6. Future Security Enhancements

As technology evolves, we continuously improve our security protocols. Future updates may include:

-  **AI-driven security monitoring** for detecting threats in real time
-  **Expanded multi-factor authentication (MFA)** for all user accounts
-  **Advanced biometric login options** for added security

Final Notes

By using ChatRx and ChatMD, you acknowledge that you have read and understood this **Data Security Policy**. We are committed to providing a **safe, private, and compliant telemedicine experience** for all users.

2-19-25