My Wellness ID: Ensuring HIPAA Compliance

My Wellness ID is built with a strong commitment to **HIPAA compliance**, ensuring that **patient health information (PHI)** is securely handled, stored, and transmitted. Below is an overview of how My Wellness ID meets HIPAA regulations:

1. User Authentication & Access Control

- **SSO Login & Secure Authentication:** Supports **Single Sign-On (SSO)** and **email-based authentication** with **multi-factor authentication (MFA)** to prevent unauthorized access.
- **Role-Based Access Control (RBAC):** Restricts data access based on user roles, minimizing exposure to PHI.

2. Data Encryption & Secure Storage

- **End-to-End Encryption:** PHI is encrypted **in transit** (**TLS 1.2/1.3**) and **at rest** (**AES-256**) to prevent unauthorized access.
- **HIPAA-Compliant Cloud Storage:** Data is securely stored within HIPAA-compliant infrastructure with strict access controls.
- **Regular Data Backups:** Ensures data integrity and quick recovery in case of incidents.

3. Secure Communication & Data Transmission

- **FHIR API Security:** Uses **OAuth 2.0** and **SMART on FHIR protocols** to securely integrate with EHR systems like **EPIC, Cerner, NextGen, and eClinicalWorks**.
- **Secure Messaging & Notifications:** Medication reminders and alerts are sent through **HIPAA-compliant channels**, ensuring confidentiality.
- **Wearable Device Data Protection:** Health data from **Apple Watch, Fitbit,** and other wearables is securely transmitted and stored.

4. Audit Logging & Monitoring

- **Activity Logs:** Tracks all user actions, including **login attempts, data access, and modifications**.
- **Intrusion Detection & Monitoring:** Implements **real-time threat monitoring** with **automated alerts** for suspicious activities.
- **Audit Trails:** Maintains a **detailed record of data access and changes** to ensure HIPAA compliance.

5. Patient Rights & Data Management

- **Data Access & Portability:** Patients can **access their health data** and request copies in accordance with HIPAA.
- **Consent Management:** Patients provide **explicit consent** for data sharing, ensuring transparency.

- **Right to be Forgotten:** Users can request **data deletion**, following HIPAA guidelines.

6. Incident Response & Breach Notification

- **Data Breach Response Plan:** A structured plan for **identifying, mitigating, and notifying** affected parties in case of a breach.
- **HIPAA-Compliant Reporting:** Ensures that any **security incident is reported** to the relevant authorities as required by HIPAA.

7. Compliance Training & Policies

- **HIPAA Training:** Regular **HIPAA compliance training** for staff and partners.
- **Policies & Procedures:** Clear policies for **handling PHI securely** and maintaining compliance.

By implementing these **robust security measures**, My Wellness ID ensures **full HIPAA compliance**, protecting user data while enabling **seamless healthcare integration**.