Application Security and Privacy Policy

Introduction Our application is committed to protecting the privacy and security of patients' health information. This document outlines how our application handles, stores, and safeguards health information retrieved through the Quanum EHR FHIR API. Our practices are fully compliant with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and applicable local privacy laws.

How We Use Health Information

1. **Purpose of Data Usage**
   - Health information is retrieved exclusively to provide the functionality and services offered by our application, such as facilitating patient care, managing health records, and generating insights for users.
   - Data will not be used for any other purpose, such as marketing or sales, without explicit patient consent.
2. **Transparency**
   - Patients will be informed about the specific health information retrieved, the purpose for accessing it, and how it will be used within the application.

How We Store Health Information

1. **Secure Storage**
   - Health information is stored using industry-standard encryption protocols (e.g., AES-256) to ensure data confidentiality.
   - Encryption is applied both at rest (in databases) and in transit (e.g., HTTPS).
2. **Limited Retention**
   - Health information is retained only for as long as necessary to fulfill the services offered by the application or as required by applicable laws.
   - Patients may request deletion of their health data at any time.
3. **Data Access Control**
   - Access to patient health information is restricted to authorized personnel and systems. Role-based access control (RBAC) is implemented to ensure users only access information they are authorized to view.

How We Protect Health Information

1. **Security Measures**
    - We implement a combination of administrative, physical, and technical safeguards to protect patient health information:
        - Regular security audits and vulnerability assessments.
        - Secure authentication mechanisms (e.g., multi-factor authentication).
        - Firewalls and intrusion detection/prevention systems.
2. **Breach Notification**
    - In the event of a data breach, patients will be notified promptly, along with relevant authorities, in compliance with applicable breach notification laws.
3. **Third-Party Services**
    - Any third-party service providers used to process or store health information are carefully vetted to ensure they meet the same security and privacy standards.

Patient Rights

1. **Right to Access**
    - Patients can request access to their health information retrieved by our application at any time.
2. **Right to Deletion**
    - Patients can request the deletion of their health information from our application.
3. **Right to Informed Consent**
    - No health information is retrieved without the patient’s explicit consent.

Compliance and Monitoring

1. **HIPAA Compliance**
    - Our application adheres to all HIPAA requirements, including the Privacy Rule, Security Rule, and Breach Notification Rule.
2. **Periodic Reviews**
    - We conduct regular reviews of our security and privacy policies to ensure compliance with evolving legal requirements and industry standards.

Contact Us

If you have any questions or concerns about our security and privacy policies, please contact us:

Email: nmadapati@gmail.com
Phone: 9095757766
Address: 13162 evening view Dr , Chino hills , Ca

Last Updated: 1/17/2025

This policy may be updated periodically to reflect changes in our practices or legal requirements. Patients will be notified of significant updates