Security & Compliance strategy

In order to make sure that the application operates with FHIR data safely and complies with HIPAA requirements, the below strategies can be suggested:

1. Authorization and authentication

- OAuth 2.0 + SMART on FHIR (Future Implementation):
  Implement SMART on FHIR combining safe, authorized, and industry-standard protocols to gain access to FHIR resources.

- Role based JWT Tokens:
  In cases of a custom or mock environment, apply JSON Web Tokens (JWT) to issue and validate roles such as admin, clinician, or viewer.

2. RBAC or Role-Based Access Control

- Role-specification of users:

  - **Admin**: Control user accounts, see all the requests.

  - **Clinician**: Send and receive queries, read patient summaries.

  - **Viewer**: The statistics of non-PHI only.

Component JWT JWT Claims Based JWT claims.

Add frontend route-level guards to obscure application backstage.

3. Privacy and Security Data
Transport Layer Security (TLS):
Communication with all channels of frontend, backend, and external FHIR APIs should be performed through HTTPS.

- **CORS Restrictions**:
  Backend API should only be called by certain origins.

- **JSON-only communication**:
  Avails foreseeable order and removes ambiguity.

- **Filtering of Input:**
  Both the frontend and backend checks all the incoming fields on their types, length, and format.

4. Auditing and logging
Access the logs /query route and all the data extracted with NLP.

Metadata on logs:

- Timestamp

- User (of JWT)

- Client IP
- FHIR bated input

Keep logs in append-only encrypted store (e.g. CloudWatch, AzureMonitor).

Future: adopt audit trail retention policy (e.g. 6 years according to HIPAA).

5. Isolation of containers & Network Segmentation
Every component has its container on Docker.

Backend APIs are not open.

Communication between the frontend and backend happens through secure bridge (backend:5000 in docker-compose).