HIPAA Compliance & Security Plan for AI on FHIR

This document outlines how I would approach HIPAA compliance and data security if this AI on FHIR application were deployed in a production environment handling real Protected Health Information (PHI).

Authentication & Authorization

- OAuth 2.0 + SMART on FHIR for secure, standards-based access control.
- Identity Management via providers like Okta or Auth0 with MFA, session timeouts, and strong password policies.

Role-Based Access Control (RBAC)

- Scoped Access based on roles (clinician, researcher, admin).
- Minimum Necessary Principle to limit data exposure.
- Patient Consent Enforcement when required by the FHIR source.

Audit Logging

- Log every PHI access: who, what, when.
- Store logs in tamper-proof systems (e.g., CloudTrail, ELK).
- Use anomaly detection to flag suspicious activity.

Data Protection

- Encryption in Transit using HTTPS (TLS 1.2+).
- Encryption at Rest via AES-256 and cloud-managed KMS.
- Data Masking in UI to hide sensitive identifiers when not required.

PHI Handling & Storage

- No PHI Stored on Frontend — all data is transient.
- Stateless Architecture — no PHI persisted or logged.
- Input Sanitization to prevent injection attacks or misuse.

Infrastructure Security

- Private VPC Deployment with restricted access via API Gateway.
- WAFs & Firewalls to block OWASP Top 10 and DDoS threats.
- Secrets Managed Securely via AWS Secrets Manager or Vault.

Continuous Monitoring & Compliance

- Backups & Disaster Recovery with encrypted, versioned snapshots.
- Automated Vulnerability Scanning using tools like Snyk.
- Access Audits to enforce least-privilege over time.

This project uses mock data, but its architecture is designed to scale securely. With the right controls in place, it can meet HIPAA requirements and safely handle PHI in production.