HIPAA Compliance and Secure FHIR Data Handling Plan

Document Prepared By: Nidhi Thakkar
Date: June 23, 2025

This document outlines a security plan to ensure that the system handling FHIR data complies with HIPAA regulations. It addresses authentication/authorization mechanisms, data privacy and audit logging strategies, and role-based access control considerations.

Authentication and Authorization Mechanisms

The system will implement OAuth 2.0 as the primary authentication and authorization framework, supplemented by SMART on FHIR for healthcare-specific integration. A centralized authorization server will issue access tokens with defined scopes, ensuring only authorized users and applications can access FHIR data. This approach provides robust token-based authentication, aligning with HIPAA's security standards for controlled access.

Data Privacy and Audit Logging Strategy

To protect FHIR data, encryption will be applied both at rest and in transit. Data at rest will utilize AES-256 encryption, while TLS 1.3 will secure data in transit. A data retention policy will limit storage to necessary periods, with secure purging of outdated records to minimize risks.

Audit logging will record all interactions with FHIR data, including user identity, timestamp, and action performed. Logs will be stored in a separate, tamper-proof database, enabling traceability and compliance with HIPAA audit requirements.

Role-Based Access Control (RBAC) Considerations

RBAC will be implemented to restrict access based on user roles, such as "Physician," "Nurse," or "Admin," each assigned specific permissions (e.g., read-only for nurses, update rights for admins). A policy engine, such as OpenPolicyAgent, will enforce these rules dynamically. Roles will be reviewed quarterly to ensure alignment with operational needs, maintaining HIPAA-compliant access controls.

Conclusion

This plan ensures HIPAA compliance by securing authentication, protecting data privacy, enabling auditability, and enforcing RBAC. The proposed measures provide a secure foundation for handling FHIR data, with flexibility for future adjustments based on system requirements or regulatory updates.