Security & Compliance Plan – AI on FHIR System

I did not think of a plan for this application and many related projects I did before in school. However, if I can have a security and compliance plan for the system, here is what I can do:

1. **Authentication & Authorization:**
    a. Should integrate system with OAuth 2.0 because it can authorize clients who obtain an access token before they can make requests on the application. Each user needs to be authorized through IdP provider such as OpenID Connect or Azure AD. I am going to use SMART features to scope specific permission as short-lived permission, validate all requests and deny any expired tokens.

2. **Data Privacy & Audit Logging:**
    a. For my understanding, the internet currently has man-in-the-middle attack mainly. So, I will use AES-256 encryption within the database. AES-256 main feature is to maintain audit logs in detail. They can capture any users who access the system and purpose of access (what they write in input?). This feature is totally immutable, stored securely as I know.

3. **Role-Based Access Control:**
    a. We need to ensure patient data security by predefining role of users (e.g., Clinician, Researcher, or Administrator). For example, administrators can have access to modify the application format, or its data. Also, clinicians should only read and write to assign patient records. Or researchers only access de-identified datasets.

Thank you for your patience!