To ensure a FHIR system is HIPAA-compliant, implement a three-pillar security strategy:

1. Authorization: Useing SMART on FHIR (based on OAuth 2.0) for secure app authentication. Mandate PKCE to prevent code interception attacks.

2. Audit Logging: Log all ePHI access attempts (who, what, when, where, outcome). Securely store these immutable logs for a minimum of six years to meet HIPAA requirements.

3. Access Control: Implement Role-Based Access Control (RBAC) to enforce the "minimum necessary" standard. Assign permissions to roles (e.g., Clinician, Billing) rather than individuals, ensuring users only access data essential to their function.