FHIR Query Tool – Security & Compliance Plan

Authentication & Authorization:
- Implement OAuth 2.0 for secure access delegation, using standards like SMART on FHIR.
- Ensure API endpoints require bearer tokens and validate them against a trusted identity provider.
- Use JWTs (JSON Web Tokens) to securely transmit user identity and scope of access.

Data Privacy & Audit Logging:
- All data transmissions are encrypted using HTTPS (TLS 1.2+).
- Sensitive fields (e.g., patient names, identifiers) are redacted from logs and only stored if necessary.
- Implement structured audit logging to track data access and changes, with timestamps, user IDs, and action types.
- Encrypt stored FHIR resources using secure algorithms like AES-256 if data is persisted.

Role-Based Access Control (RBAC):
- Define roles: e.g., admin, clinician, researcher.
- Each role has specific data access privileges.
- Use middleware to enforce access restrictions based on user role and resource type.
- Patient-identifiable information is only accessible by authorized roles.