**Security Architecture Document**

**Purpose**: Outlines the system’s approach to safeguarding data and ensuring compliance.

**Components**:

* **Authentication & Authorization**:
  + Multi-factor authentication (2FA)
  + RBAC model
* **Encryption**:
  + AES-256 for data at rest
  + TLS 1.3 for all in-transit communications
* **Data Protection**:
  + Regular database backups
  + Anonymization for PII data during export
* **Auditing & Monitoring**:
  + Centralized logging (e.g., ELK stack)
  + Intrusion detection system (IDS) integration
* **Compliance Standards**:
  + GDPR, Sphere Humanitarian Standards, ISO/IEC 27001
* **Incident Response**:
  + Playbook for breaches
  + 24h response window with escalation matrix