1. **Data Encryption and Anonymization Plan**
   1. **Data Encryption Approach**

* **Data In Transit (During Transmission):**

All user and system data transfers will be protected by TLS 1.3 (HTTPS) encryption methods. SSL/TLS certificates will be provided to the web servers (like NGINX) so that secure connections can be made. All non-secure connections will be rejected by API services, which will only work with HTTPS queries. Secure internal communication between backend services and administrators occurs through VPN tunnel technology.

* **Data at Rest (Stored Data):**

MongoDB and MySQL store patient records and billing information with AES-256 encryption to protect sensitive data. The PACS system (DICOM files) stores MRI images by utilizing disk-level or file-based encryption methods. The encryption keys will be stored and managed through a Key Management Service (KMS) which grants access only to authorized processes.

* **Password Security:**

All user passwords will be protected through the bcrypt hashing method which prevents plain text storage and transmission.

* **Access Control and Auditing:**

The system will implement Role-Based Access Control (RBAC) to grant users access only to required functions. All system user activities will be recorded in encrypted audit trails that serve both monitoring and compliance needs.

**12.2 Data Anonymization Strategy**

**Purpose:**

User privacy protection through anonymization techniques will be used for both testing and research purposes as well as data sharing with external parties.

**Methods:**

* The system will use data masking to replace personal details (e.g., names and contact information) with general substitutes in environments other than production.
* Patient records will receive pseudo-identifiers through pseudonymization which enables controlled re-identification without exposing direct patient identity information.
* Analytical reports use aggregated data statistics (such as total scan numbers) instead of revealing individual patient records.
* The removal of metadata from DICOM images occurs when the images are used outside clinical environments.

**Re-Identification Control:**

Admins possess the only authorization to perform pseudonymization reversals when medical requirements exist through secure access channels.