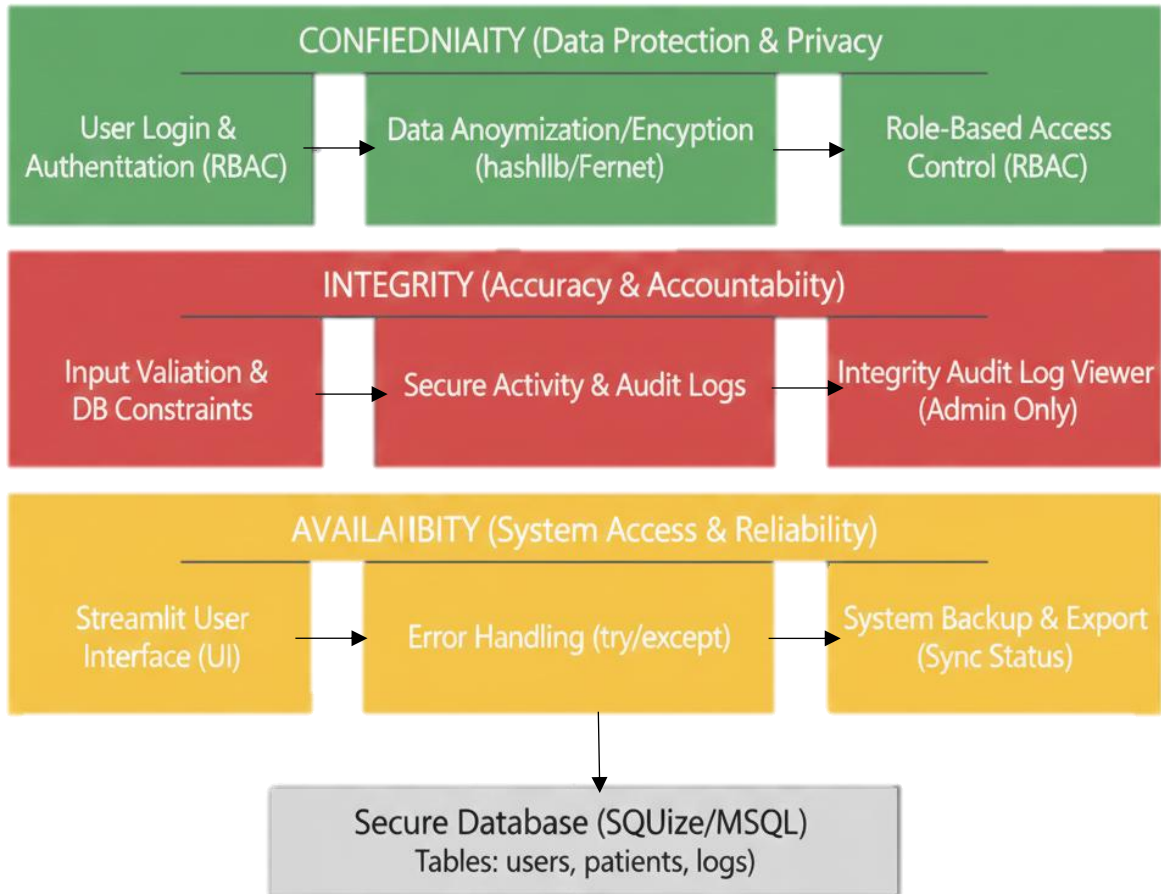Talha Durrani

# GDPR-Compliant Hospital Management System

Lawful, Fair, Transparent Processing
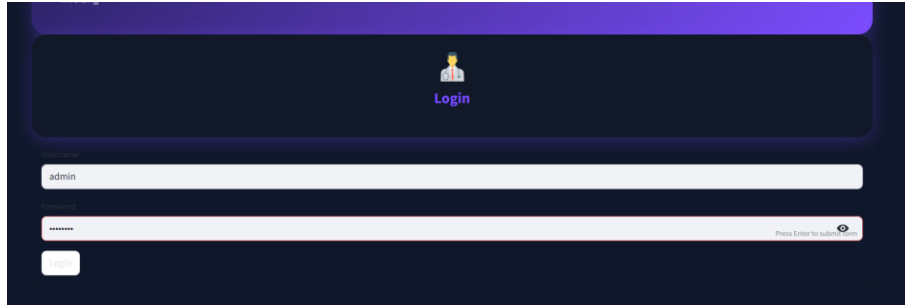
Talha Durrani – 22K-4144

Asadullah – 22K-4138

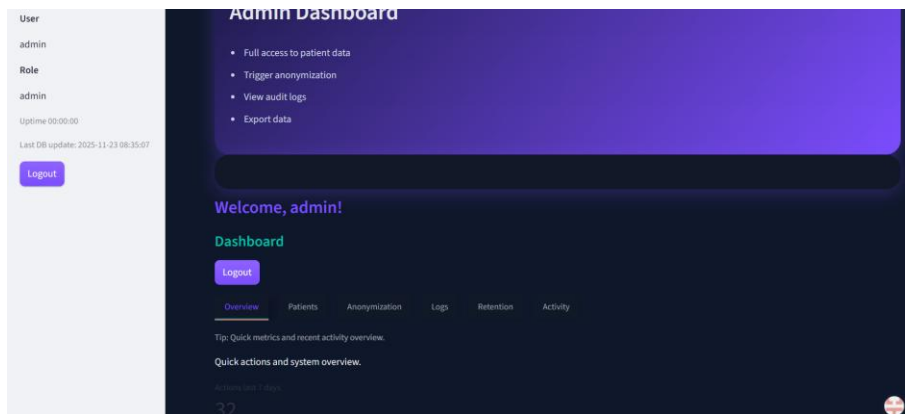# System Overview Diagram



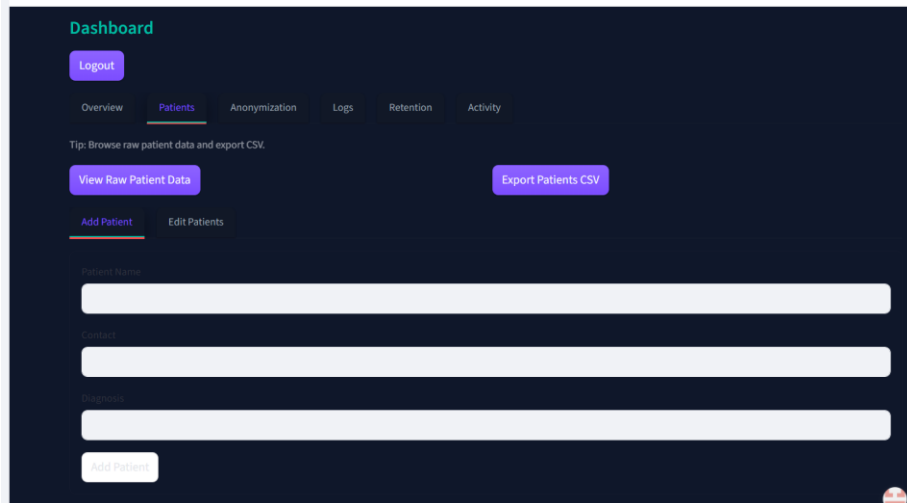**CONFIEDNIAITY (Data Protection & Privacy**

| User Login & Authentitation (RBAC) | → Data Anoymization/Encyption (hashllb/Fernet) | → Role-Based Access Control (RBAC) |

**INTEGRITY (Accuracy & Accountabiity)**

| Input Valiation & DB Constraints | → Secure Activity & Audit Logs | → Integrity Audit Log Viewer (Admin Only) |

**AVAILAIIBITY (System Access & Reliability)**

| Streamlit User Interface (UI) | → Error Handling (try/except) | → System Backup & Export (Sync Status) |

**Secure Database (SQUize/MSQL)**
Tables: users, patients, logs)

# Screenshots

## Login Page



## Admin Dashboard



## Admin's Right to Access

# Admin's Anonimization rights

**Welcome, admin!**

**Dashboard**

Logout

| Overview | Patients | Anonymization | Logs | Retention | Activity |

Tip: Apply masking or encryption, decrypt, and view anonymized data.

**Mask, encrypt, decrypt, and view anonymized patient data.**

Anonymize Patient Data (Mask)          Anonymize Patient Data (Encrypt)

Decrypt Patient Data

View Anonymized Patient Data

# Raw

View Raw Patient Data          Export Pat

| | patient_id | name | contact | diagnosis | anonymized_name | an |
|---|---|---|---|---|---|---|
| 0 | 1 | John Doe | 123-456-7890 | Flu | John Doe | 12 |
| 1 | 2 | Jane Smith | 987-654-3210 | Diabetes | Jane Smith | 98 |
| 2 | 3 | Asad | 12347891111 | flu | Asad | 12 |
| 3 | 4 | Asad | 12347891111 | flu | Asad | 12 |
| 4 | 5 | john | 9276428864 | GIT Infection | None | N |

Add Patient          Edit Patients

## Masked



## Encrypted

# Audit Logs

Overview | Patients | Anonymization | **Logs** | Retention | Activity

Tip: Review audit logs and export for compliance.

**View Audit Log**                    ⬇ 🔍 ⛶          **Export Logs CSV**

| | log_id | user_id | role | action | timestamp | |
|---|---|---|---|---|---|---|
| 61 | 62 | 1 | admin | anonymization | 2025-11-23T08:51:40.158039 | |
| 62 | 63 | 1 | admin | anonymization | 2025-11-23T08:51:41.159879 | |
| 63 | 64 | 1 | admin | anonymization | 2025-11-23T08:51:45.208858 | |
| 64 | 65 | 1 | admin | anonymization | 2025-11-23T08:51:49.096070 | |
| 65 | 66 | 1 | admin | decryption | 2025-11-23T08:51:52.126963 | |
| 66 | 67 | 1 | admin | anonymization | 2025-11-23T08:51:56.986796 | |
| 67 | 68 | 1 | admin | anonymization | 2025-11-23T08:52:14.394854 | |
| 68 | 69 | 1 | admin | decryption | 2025-11-23T08:52:15.735958 | |
| 69 | 70 | 1 | admin | anonymization | 2025-11-23T08:52:18.839363 | |
| 70 | 71 | 1 | admin | edit_patient | 2025-11-23T08:52:34.201985 | |

# Retention Rights

Data Retention (Admin)

Retention days (soft-delete patients older than this). Use 0 to purge all

| 0 | − + |
|---|---|

**Purge (soft-delete) patients older than retention**

Download archive CSV of purged patients

Soft-deleted 9 patients and provided CSV archive.

☑ I understand this will permanently delete soft-deleted patient records

**Permanently delete soft-deleted patients**

Download archive CSV (permanent delete)

Permanently deleted 9 patients. Archive CSV available for download above.

**Generate demo old patients (for retention test)**

**Welcome, admin!**

**Dashboard**

**Logout**

Overview | Patients | Anonymization | Logs | Retention | Activity

Tip: Browse raw patient data and export CSV.

**View Raw Patient Data**                    **Export Patients CSV**

| | patient_id | name | contact | diagnosis | anonymized_name | anonymized_co |
|---|---|---|---|---|---|---|
| | | | | empty | | |

Add Patient | Edit Patients

# Activity Graph:
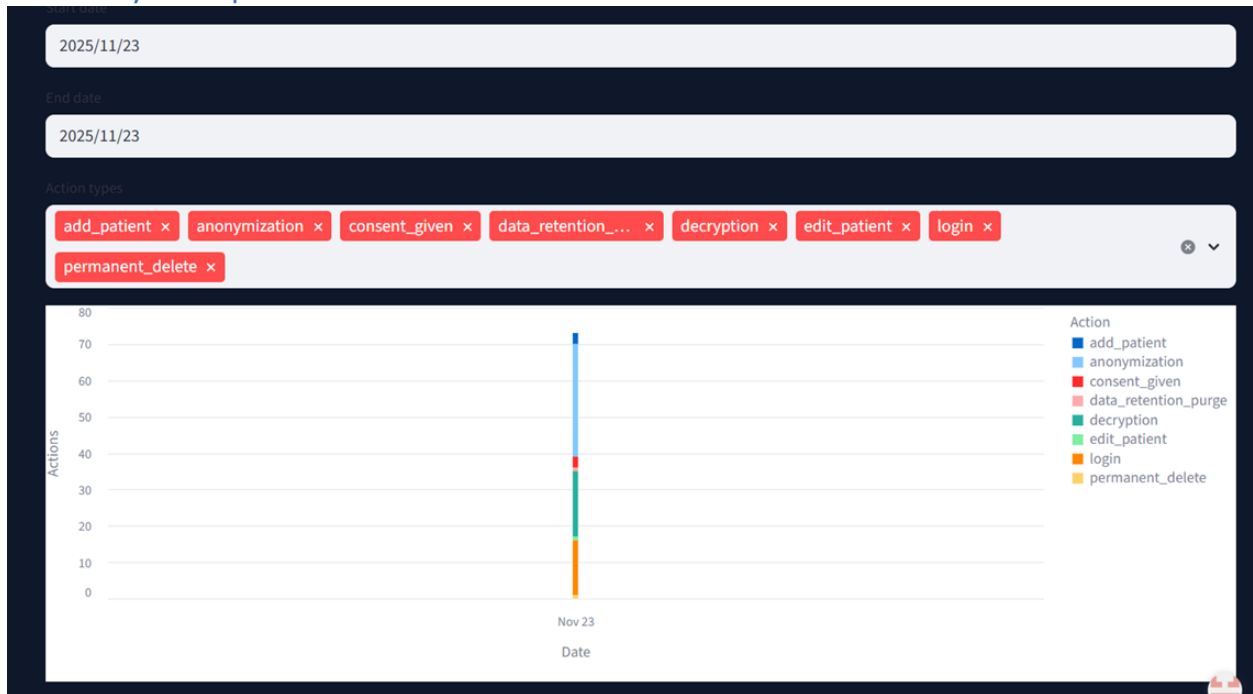


# Receptionist Dashboard:

# Doctor Dashboard:
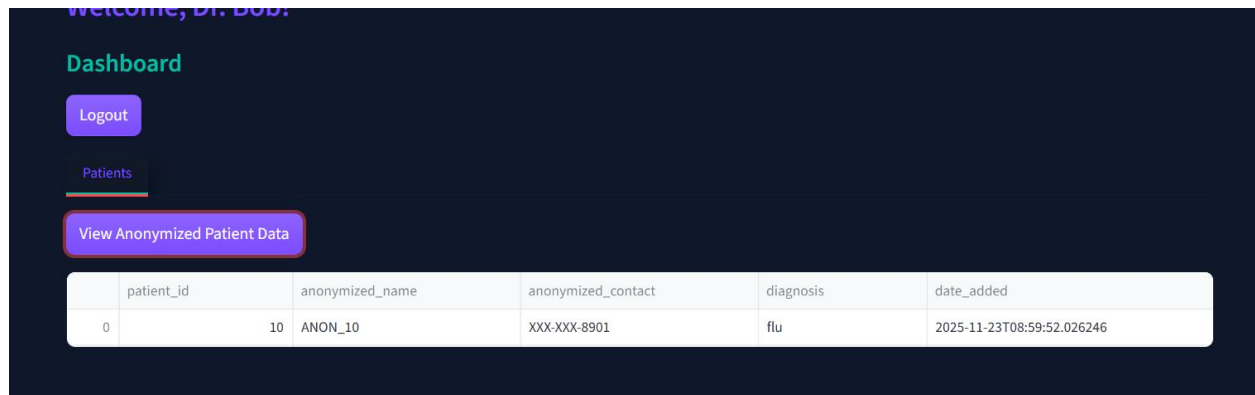


# Discussion: CIA Triad & GDPR Implementation

## Confidentiality:

- Patient names, contacts, and diagnoses are anonymized using hashing or masking.
- Role-Based Access Control ensures only Admins view raw data.
- Doctors and receptionists see restricted or anonymized data only.

## Integrity:

- All actions are logged with timestamp, role, and description.
- Database constraints and code-level checks prevent unauthorized edits.
- Admins can audit logs to ensure accountability.

## Availability:

- System includes error handling to prevent crashes.
- Database remains accessible through stable Streamlit queries.
- Backup/export (CSV) option ensures recoverability.
- System uptime or last sync time shown in footer.

## GDPR Allignment:

- Data minimization via anonymization and restricted views.
- Lawful and transparent processing through logs and RBAC.
- Consent banner, retention timers, reversible encryption (Fernet).

[Demo Video link](#)