

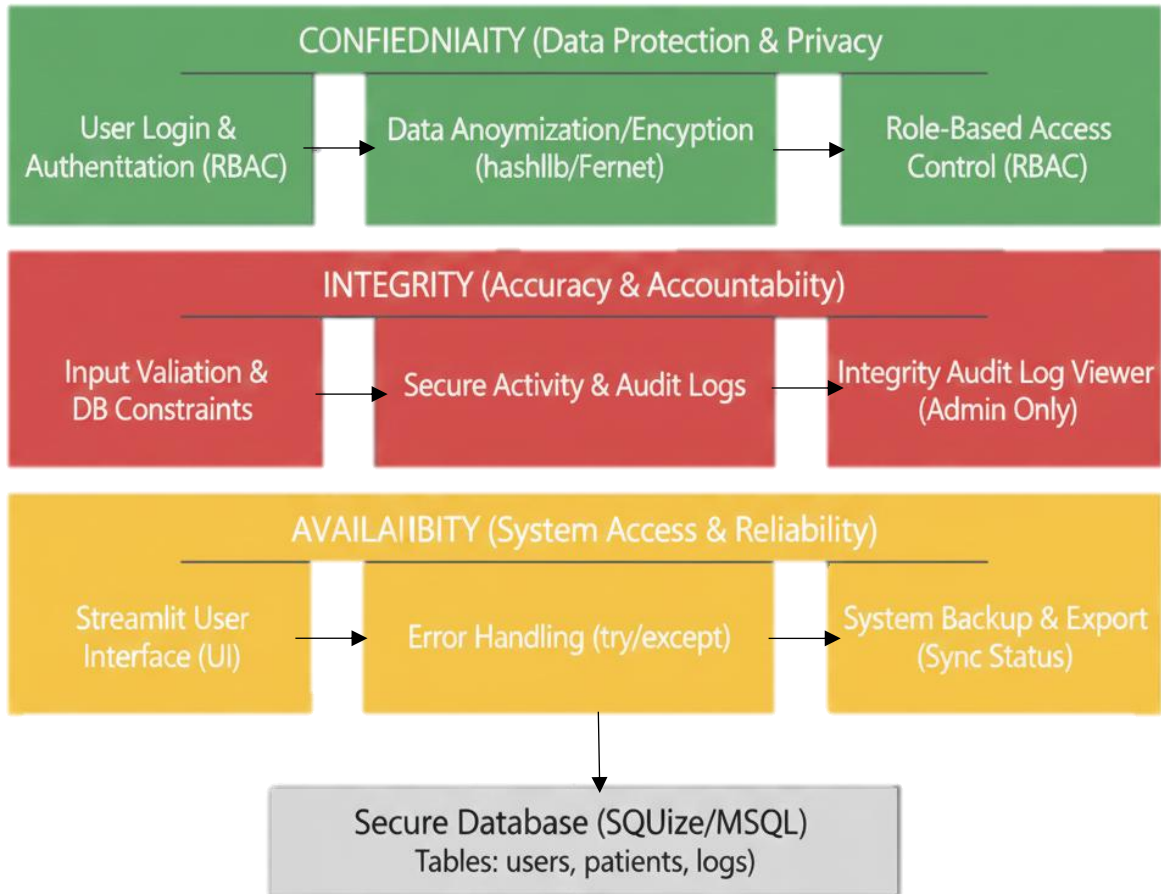
Talha Durrani

GDPR-Compliant Hospital Management System

Lawful, Fair, Transparent Processing

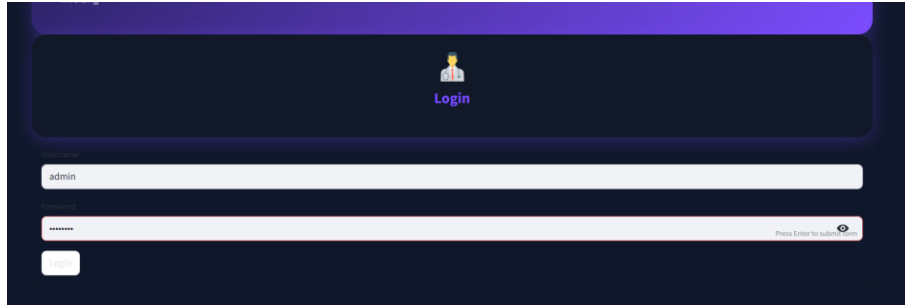
Talha Durrani – 22K-4144
Asadullah – 22K-4138

System Overview Diagram



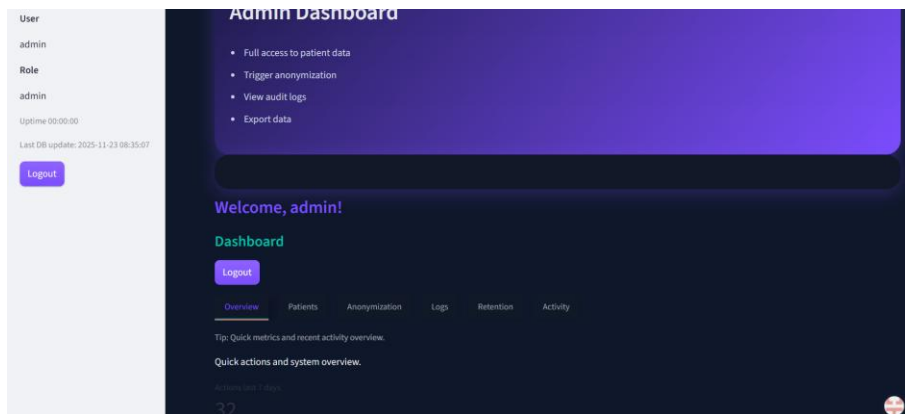
Screenshots

Login Page



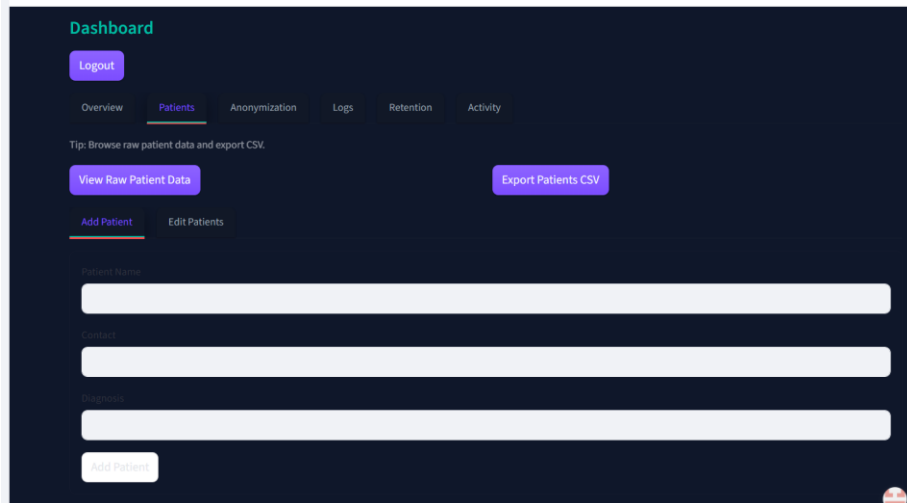
A dark-themed login page with a purple header. In the center, there is a white box containing a user icon and the word "Login". Below this, there are two input fields: the first is labeled "Username" and contains the text "admin"; the second is labeled "Password" and contains a masked password "*****". To the right of the password field, there is a small eye icon and the text "Press Enter to submit". At the bottom left of the form area, there is a "Login" button.

Admin Dashboard



The Admin Dashboard is divided into a left sidebar and a main content area. The sidebar, on the left, displays the user's name "User: admin", role "Role: admin", and system status "Uptime: 00:00:00" and "Last DB update: 2025-11-23 08:35:07". It also features a "Logout" button. The main content area has a purple header with the title "Admin Dashboard" and a list of permissions: "Full access to patient data", "Trigger anonymization", "View audit logs", and "Export data". Below the header, a "Welcome, admin!" message is followed by a "Dashboard" section with a "Logout" button. A navigation bar includes links for "Overview", "Patients", "Anonymization", "Logs", "Retention", and "Activity". A tip states: "Tip: Quick metrics and recent activity overview." Below this, it says "Quick actions and system overview." and "Automatically 12 days". At the bottom, there is a "32" and a small circular icon.

Admin's Right to Access



This form is part of the Admin's Right to Access section. It features a "Dashboard" header with a "Logout" button. Below the header, there is a navigation bar with links for "Overview", "Patients", "Anonymization", "Logs", "Retention", and "Activity". A tip states: "Tip: Browse raw patient data and export CSV." Below this, there are two buttons: "View Raw Patient Data" and "Export Patients CSV". Underneath, there are two sub-sections: "Add Patient" and "Edit Patients". The "Add Patient" section contains three input fields labeled "Patient Name", "Contact", and "Diagnosis". At the bottom left of this section, there is an "Add Patient" button. At the bottom right, there is a small circular icon.

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 Patient Data](#)

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

[Add Patient](#)[Edit Patients](#)

Masked

View Raw Patient Data

Download Search Expand

	name	contact	diagnosis	anonymized_name	anonymized_c
0	John Doe	123-456-7890	Flu	ANON_1	XXX-XXX-7890
1	Jane Smith	987-654-3210	Diabetes	ANON_2	XXX-XXX-3210
2	Asad	12347891111	flu	ANON_3	XXX-XXX-1111
3	Asad	12347891111	flu	ANON_4	XXX-XXX-1111
4	john	9276428864	GIT Infection	ANON_5	XXX-XXX-8864

Encrypted

Tip: Browse raw patient data and export CSV.

View Raw Patient Data

Download Search Expand

	name	contact	diagnosis	anonymized_name
0	John Doe	123-456-7890	Flu	gAAAAABplsjpgp6AIED0RSEJxArHpsEF
1	Jane Smith	987-654-3210	Diabetes	gAAAAABplsjsxwqEvPui-DSwjtYumwKX
2	Asad	12347891111	flu	gAAAAABplsawl83qTXxWXdoldAaKZpkS
3	Asad	12347891111	flu	gAAAAABplsjeQ_EbAyeUNFesh8D9HZO
4	John	9276428864	GIT Infection	gAAAAABplsjeSMoch2wg_A001aATNeR

Audit Logs

Logout

OverviewPatientsAnonymizationLogsRetentionActivity

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 planning

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

OverviewPatientsAnonymizationLogsRetentionActivity

Tip: Browse raw patient data and export CSV.

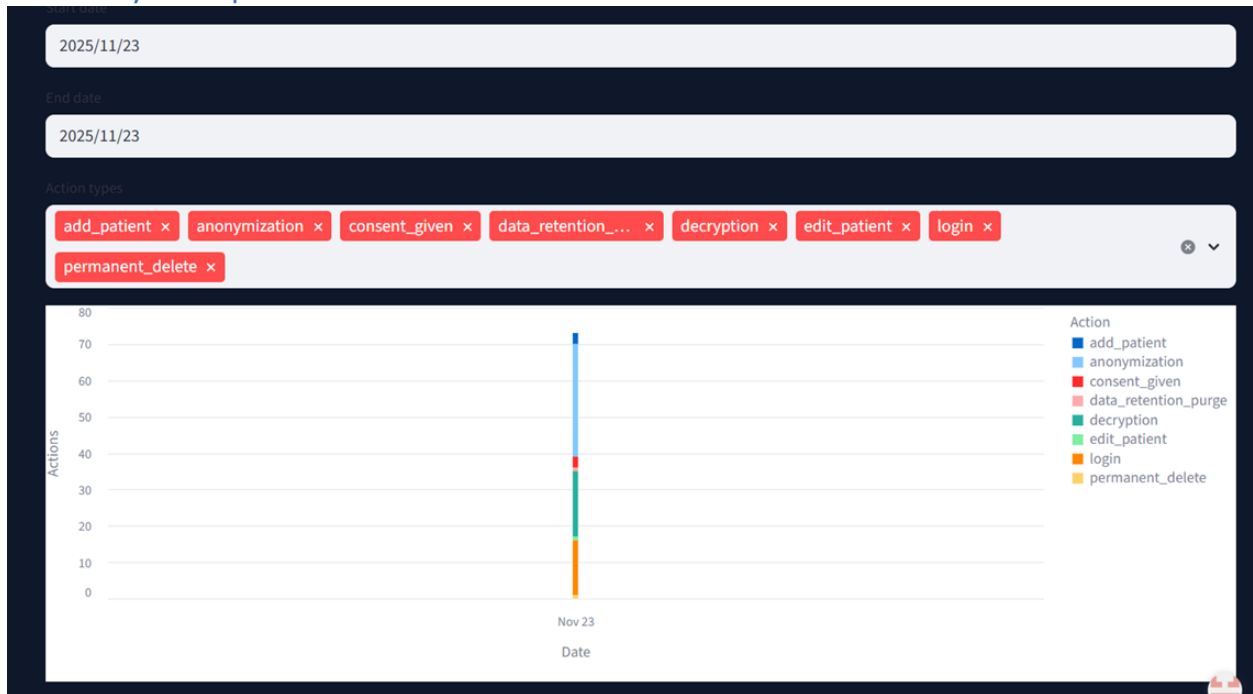
View Raw Patient Data

Export Patients CSV

patient_id	name	contact	diagnosis	anonymized_name	anonymized_co
empty					

Add PatientEdit Patients

Activity Graph:



Receptionist Dashboard:

Welcome, Alice_recep!

Dashboard

[Logout](#)

[Add Patient](#) [Edit Patients](#)

Patient Name: asad

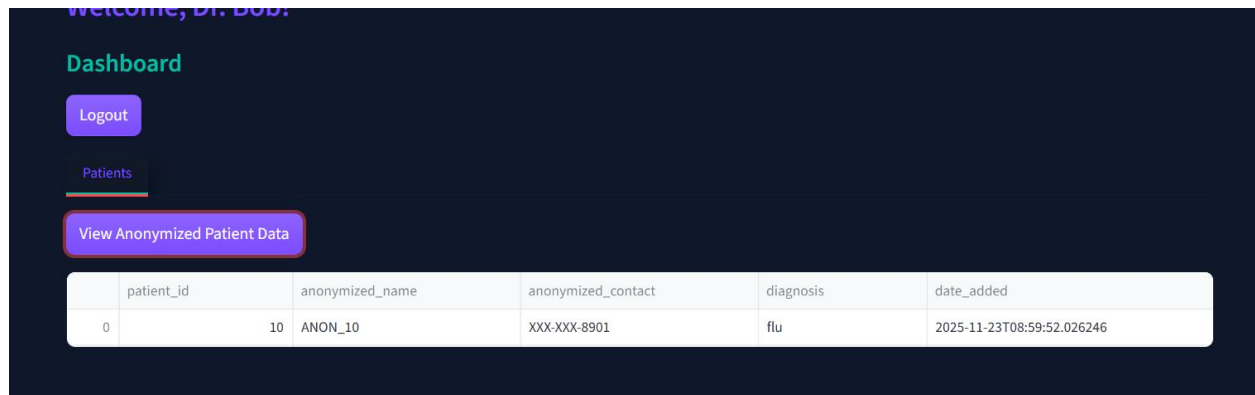
Contact: 12345678901

Diagnosis: fever

[Add Patient](#)

Patient added successfully.

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 Alignment:

- 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](#)