

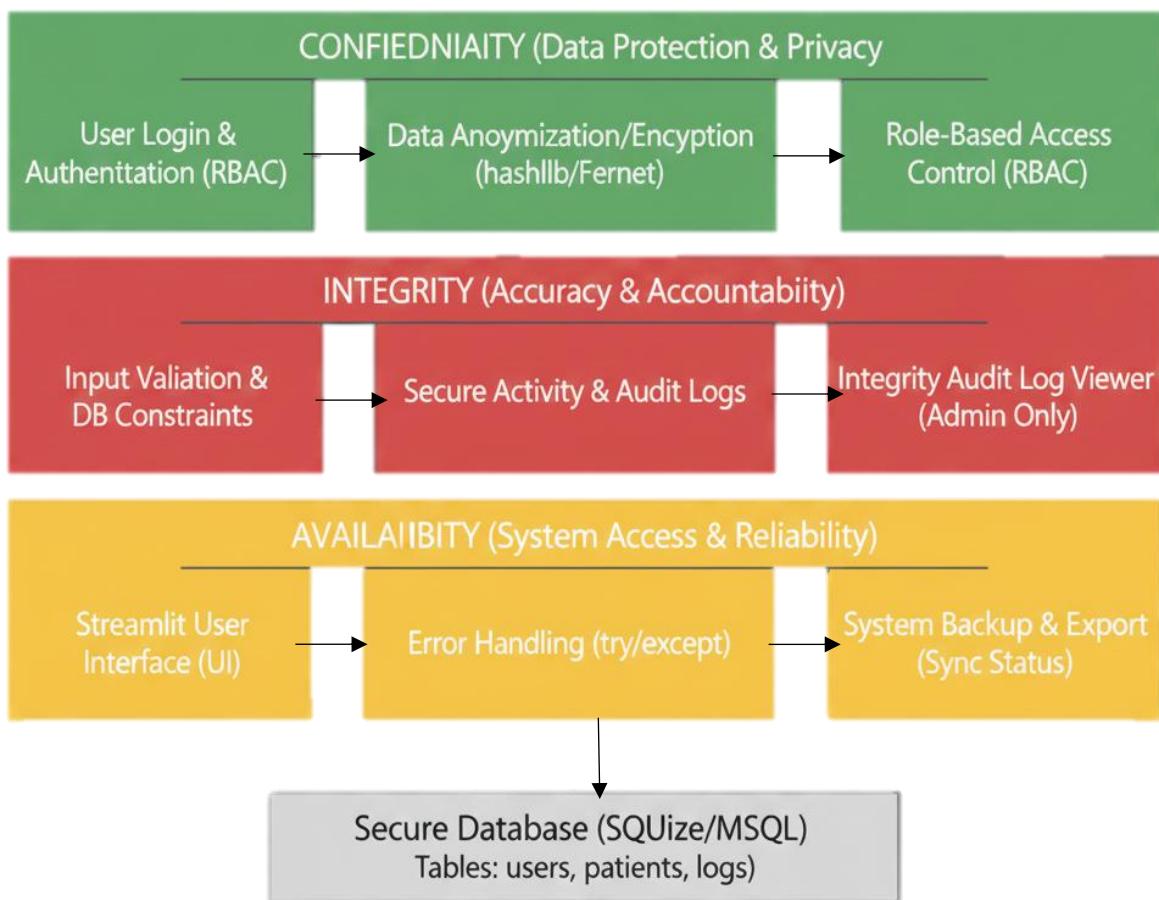
Talha Durrani

GDPR-Compliant Hospital Management System

Lawful, Fair, Transparent Processing

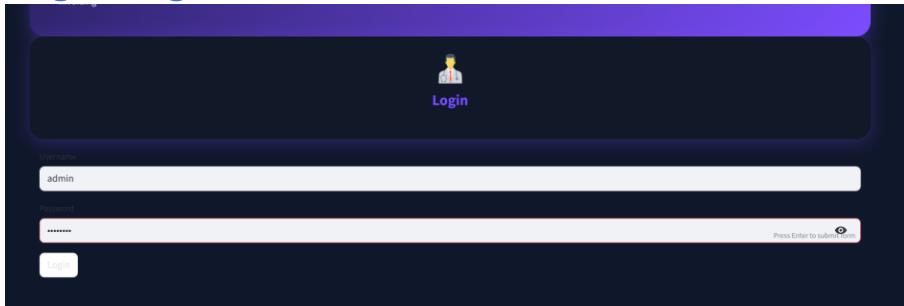
Talha Durrani – 22K-4144
Asadullah – 22K-4138

System Overview Diagram



Screenshots

Login Page



Admin Dashboard

A screenshot of the Admin Dashboard. At the top is a purple header bar with the text 'Admin Dashboard'. Below it is a dark blue background. On the left, there's a sidebar with 'User' and 'admin' listed under 'Role'. In the center, there's a 'Welcome, admin!' message, a 'Logout' button, and a navigation menu with tabs: Overview, Patients, Anonymization, Logs, Retention, and Activity. Below the navigation menu is a tip: 'Tip: Quick metrics and recent activity overview.' and a section for 'Quick actions and system overview.' with a 'Actions last 7 days.' button and a '32' badge.

Admin's Right to Access

A screenshot of the Patient Management Dashboard. At the top is a purple header bar with the text 'Dashboard'. Below it is a dark blue background. On the left, there's a sidebar with 'Logout' and tabs: Overview, Patients, Anonymization, Logs, Retention, and Activity. The 'Patients' tab is active. In the center, there are buttons for 'View Raw Patient Data' and 'Export Patients CSV'. Below them are sections for 'Add Patient' and 'Edit Patients'. There are form fields for 'Patient Name', 'Contact', and 'Diagnosis', each with a corresponding input field. At the bottom is a 'Add Patient' button.

Admin's Anonimization rights

Welcome, admin!

Dashboard

[Logout](#)

Overview Patients **Anonymization** Logs Retention Activity

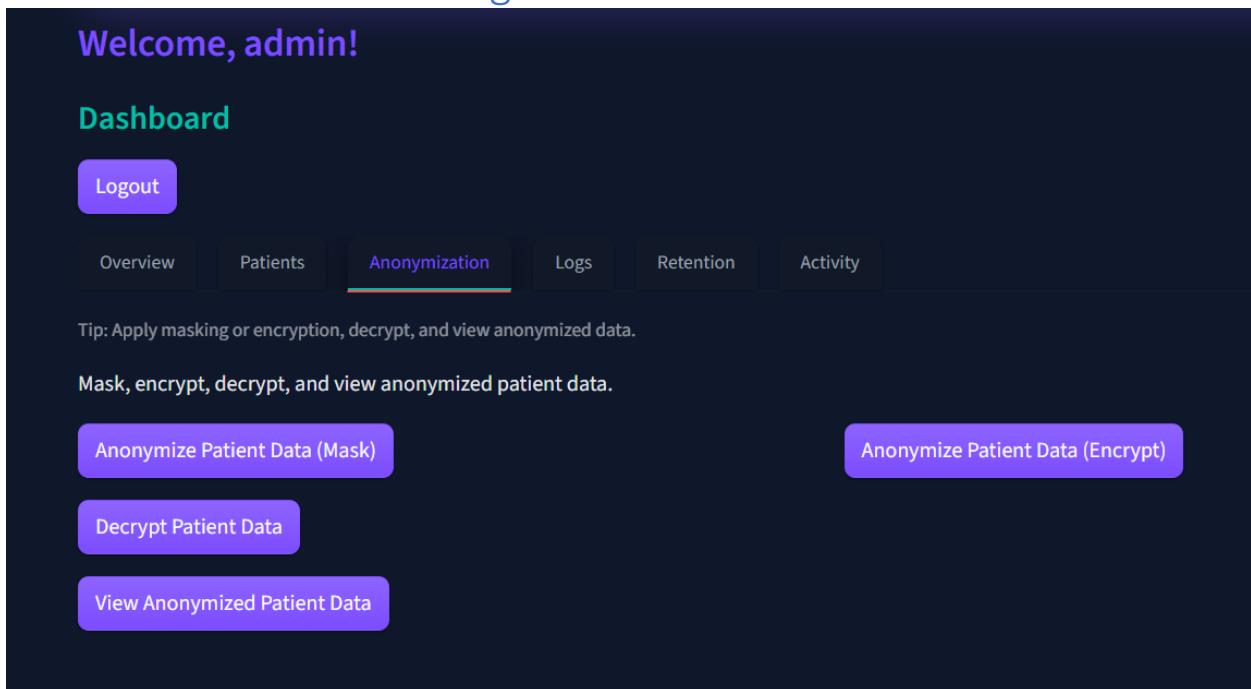
Tip: Apply masking or encryption, decrypt, and view anonymized data.

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

[Anonymize Patient Data \(Mask\)](#) [Anonymize Patient Data \(Encrypt\)](#)

[Decrypt Patient Data](#)

[View Anonymized Patient Data](#)

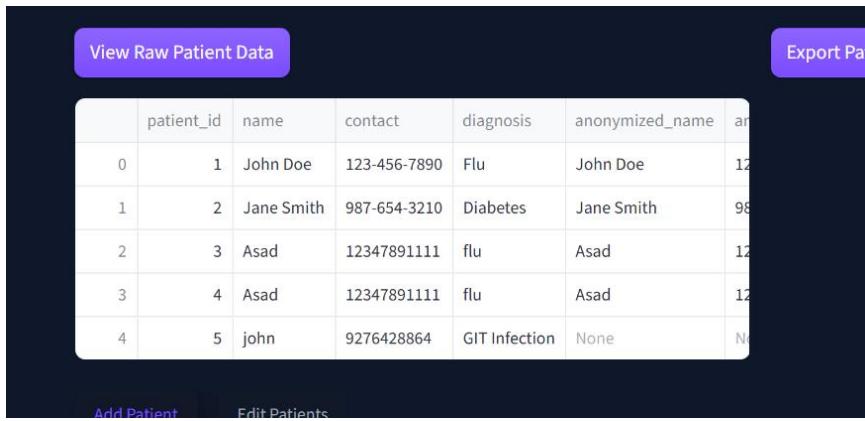


Raw

[View Raw Patient Data](#) [Export Pat](#)

	patient_id	name	contact	diagnosis	anonymized_name	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

A screenshot of a web-based application interface. At the top, there is a purple header bar with the text "View Raw Patient Data" on the left and "Export" on the right. Below this is a dark blue header with a search bar containing icons for download, search, and refresh. The main content area is a table with the following columns: name, contact, diagnosis, anonymized_name, and anonymized_c. The table has 5 rows. Row 4's contact cell is highlighted with a red border. The data is as follows:

	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

A screenshot of the same web-based application interface after the data has been encrypted. The layout is identical to the "Masked" version. The contact column for row 4 is still highlighted with a red border. The data is now encrypted, appearing as long strings of characters. The original values from the masked version are present but obscured by encryption.

	name	contact	diagnosis	anonymized_name	anonymized_c
0	John Doe	123-456-7890	Flu	gAAAAABplsjwmgp6AlED0RSEJxArHpsEF	
1	Jane Smith	987-654-3210	Diabetes	gAAAAABplsjwxwuqEvPui-DSwjItYumwKX	
2	Asad	12347891111	flu	gAAAAABplsjwl83qTxWxeDoldAaKZpkS9	
3	Asad	12347891111	flu	gAAAAABplsjweQ_EbAyeUNFEsh8D9HZO	
4	hn	9276428864	GIT Infection	gAAAAABplsjweSMoch2wg_A001aATNeR	

Audit Logs

The screenshot shows the 'Logs' tab selected in the navigation bar. A tip at the top says 'Tip: Review audit logs and export for compliance.' Below is a table titled 'View Audit Log' with columns: log_id, user_id, role, action, and timestamp. The table contains 10 rows of audit log data.

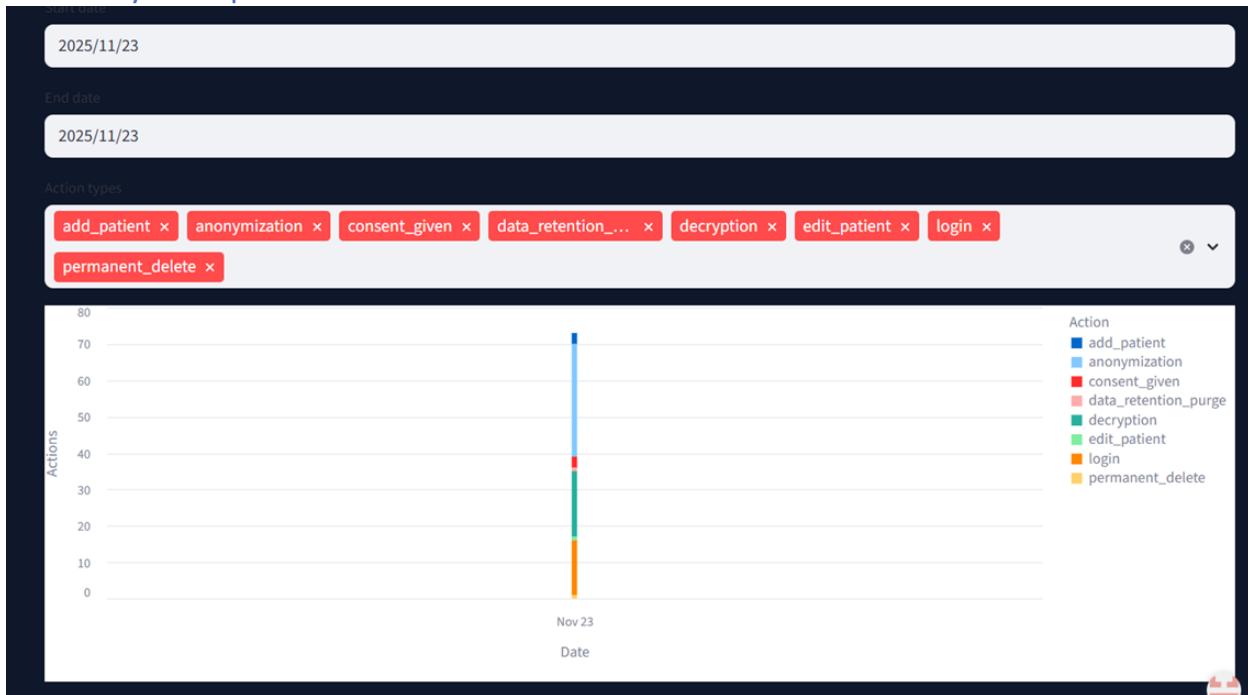
log_id	user_id	role	action	timestamp
61	62	1	admin	anonymization 2025-11-23T08:51:40.158039
62	63	1	admin	anonymization 2025-11-23T08:51:41.159879
63	64	1	admin	anonymization 2025-11-23T08:51:45.208858
64	65	1	admin	anonymization 2025-11-23T08:51:49.096070
65	66	1	admin	decryption 2025-11-23T08:51:52.126963
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

Buttons include 'View Audit Log' and 'Export Logs CSV'.

Retention Rights

The screenshot shows the 'Retention' tab selected in the navigation bar. It includes a 'Data Retention (Admin)' section with a retention age input field set to 0. Below is a 'Purge (soft-delete) patients older than retention' button, a 'Download archive CSV of purged patients' button, and a note about soft-deleted patients. A checkbox for permanent deletion is checked, followed by a 'Permanently delete soft-deleted patients' button and a 'Download archive CSV (permanent delete)' button. A success message states 'Permanently deleted 9 patients. Archive CSV available for download above.' Below is a 'Generate demo old patients (for retention test)' button. At the bottom, a welcome message 'Welcome, admin!' is displayed, along with a 'Logout' button and a navigation bar with tabs: Overview, Patients (selected), Anonymization, Logs, Retention, and Activity. A tip at the bottom says 'Tip: Browse raw patient data and export CSV.' Buttons include 'View Raw Patient Data' and 'Export Patients CSV'.

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:

The screenshot shows a Streamlit dashboard titled "Doctor Dashboard". At the top, it says "Welcome, Dr. Bob!". Below the title, there's a "Logout" button and a "Patients" tab, which is currently selected. A purple button labeled "View Anonymized Patient Data" is highlighted. Below this, a table displays a single patient record with the following data:

	patient_id	anonymized_name	anonymized_contact	diagnosis	date_added
0	10	ANON_10	XXX-XXX-8901	flu	2025-11-23T08:59:52.026Z

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](#)