INFORMATION SECURITY ASSIGNMENT - 4

Hospital Privacy Dashboard — GDPR & CIA Compliance Report

Author: Anshah Khan

Roll No: 23K-2053

---

1. Introduction

This project implements a **GDPR-compliant hospital privacy dashboard** using Python Streamlit. It securely manages patient data while providing fine-grained role-based access control. The system demonstrates the application of **Confidentiality, Integrity, and Availability (CIA)** principles and aligns with GDPR guidelines for data protection.

Key Features:

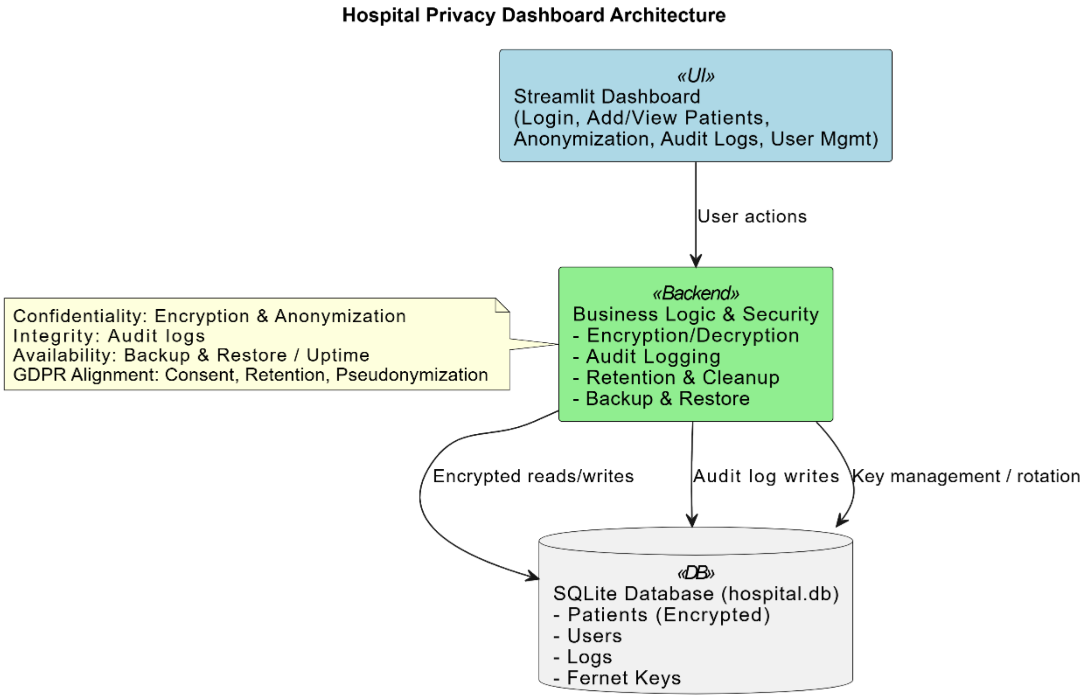
- Role-based access (Admin, Doctor, Receptionist)
- Encryption of sensitive fields using **Fernet symmetric encryption**
- Anonymization of patient identifiers (name, contact)
- Audit logs for all system actions
- Data retention policies
- Backup & restore with key versioning

---

2. System Overview

2.1 Architecture Diagram

Below is a conceptual diagram showing **CIA layers** implemented in the system:


Hospital Privacy Dashboard Architecture
«UI»
Streamlit Dashboard
(Login, Add/View Patients,
Anonymization, Audit Logs, User Mgmt)
User actions
«Backend»
Business Logic & Security
- Encryption/Decryption
- Audit Logging
- Retention & Cleanup
- Backup & Restore
Confidentiality: Encryption & Anonymization
Integrity: Audit logs
Availability: Backup & Restore / Uptime
GDPR Alignment: Consent, Retention, Pseudonymization
Encrypted reads/writes
Audit log writes
Key management / rotation
«DB»
SQLite Database (hospital.db)
- Patients (Encrypted)
- Users
- Logs
- Fernet Keys

Explanation:

- **Confidentiality:** Sensitive patient fields (name, contact) are encrypted using Fernet. Admins can re-encrypt data after key rotation.
- **Integrity:** Audit logs record all actions (login, patient edits, anonymization) to ensure traceability and tamper detection.
- **Availability:** Regular backups and system uptime tracking ensure data remains available. Auto-refresh monitors system status.

---

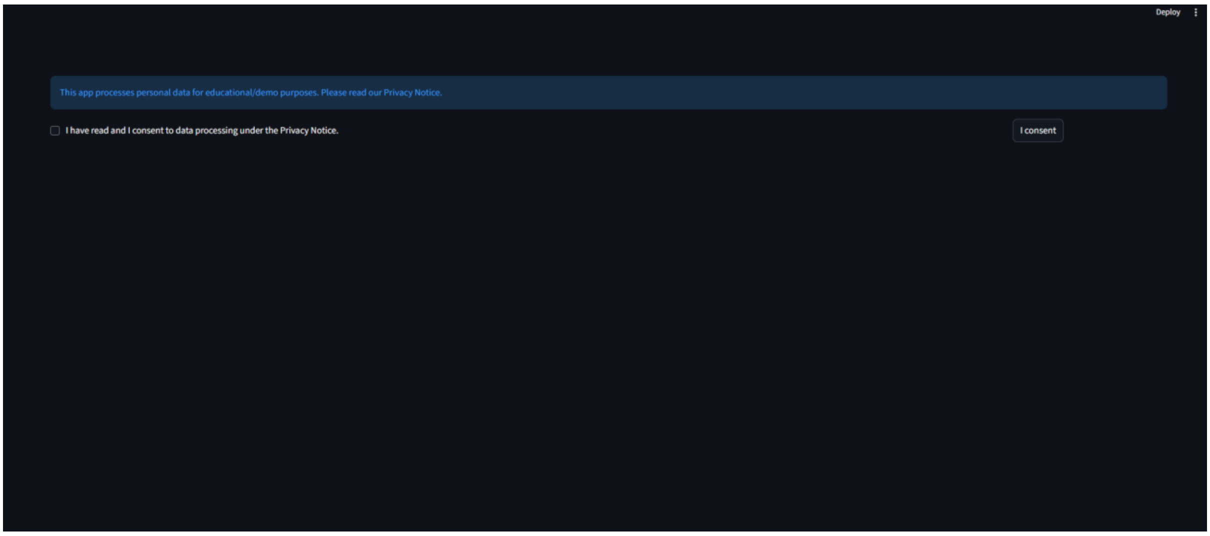
3. Key Functional Screens

This section highlights the main user interfaces and functionalities of the Hospital Privacy Dashboard, including screenshots for demonstration.

3.1 Consent Screen

- Displays GDPR consent banner before login.
- Users must confirm they accept the privacy notice.
- Consent is logged for audit purposes.

Screenshot:



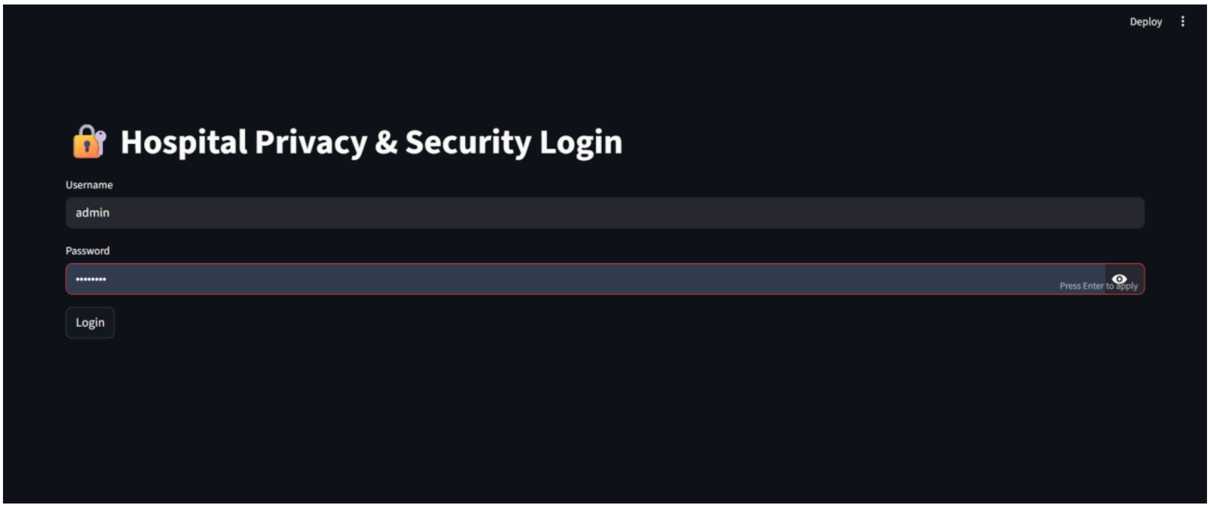
This app processes personal data for educational/demo purposes. Please read our Privacy Notice.

□ I have read and I consent to data processing under the Privacy Notice.

3.2 Login Screen

- Users authenticate using username/password.
- Role-based access enforced:
  - Admin: Full access
  - Doctor: Limited patient data (anonymized)
  - Receptionist: Basic access (diagnosis, scheduling)
- Successful login triggers audit log entry.

Screenshot:



🔐 Hospital Privacy & Security Login

Username: admin

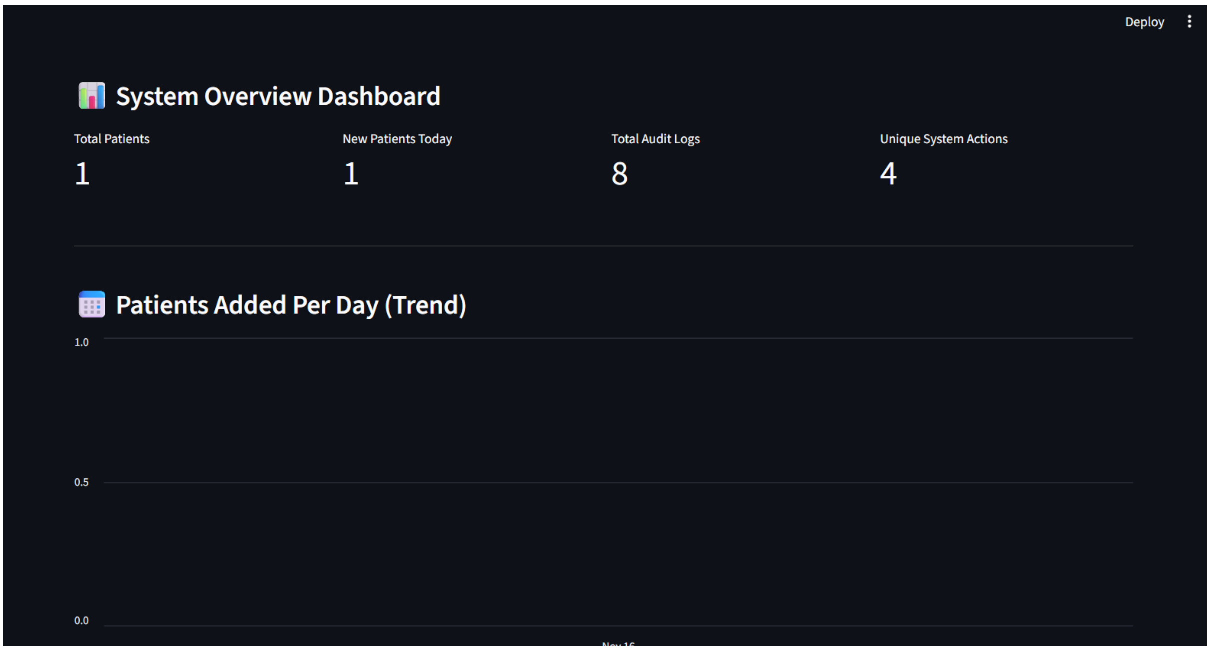
Password: ••••••••

3.3 Dashboard / Home

- Displays system overview for the logged-in user.

- Admin view includes:
  - Total patients
  - New patients today
  - Total audit logs
  - Unique system actions
- Auto-refresh for real-time uptime display.

Screenshot:



System Overview Dashboard

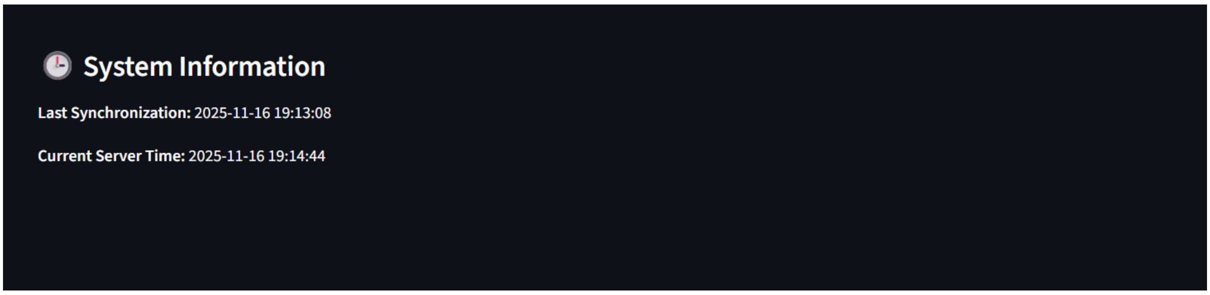
Total Patients 1

New Patients Today 1

Total Audit Logs 8

Unique System Actions 4

Patients Added Per Day (Trend)



System Information

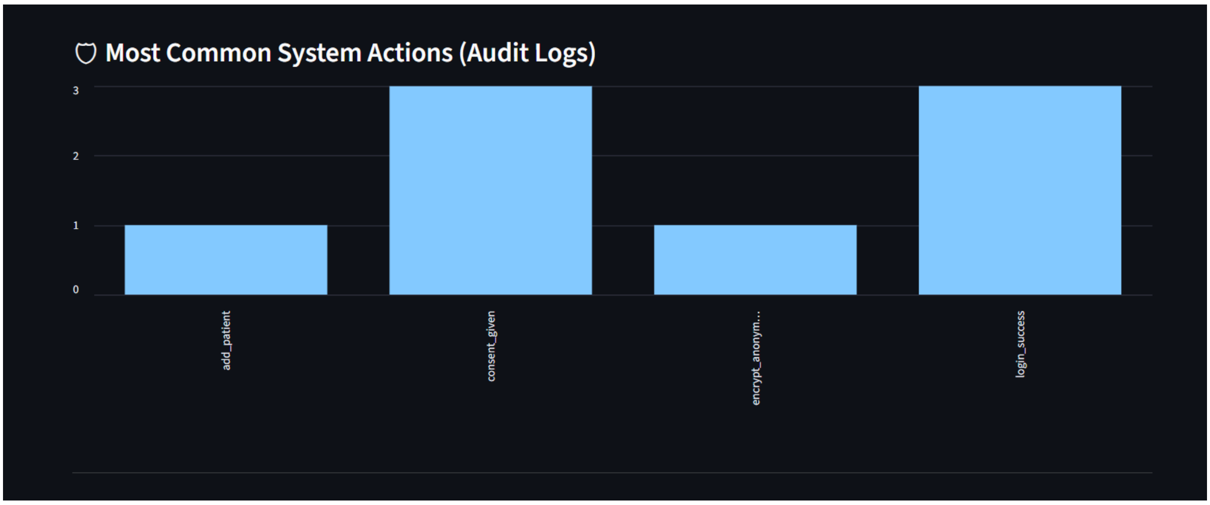
Last Synchronization: 2025-11-16 19:13:08

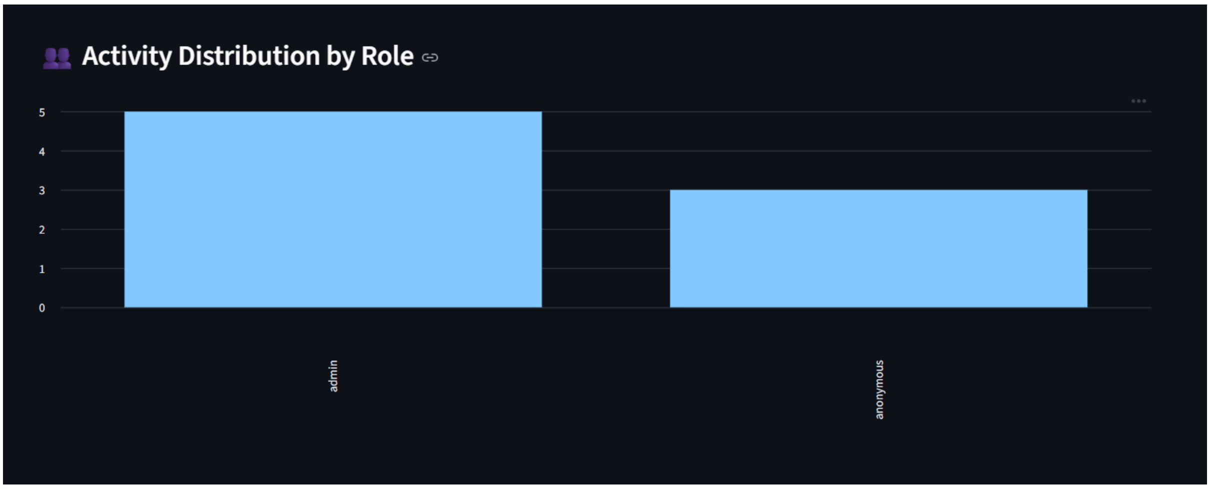
Current Server Time: 2025-11-16 19:14:44

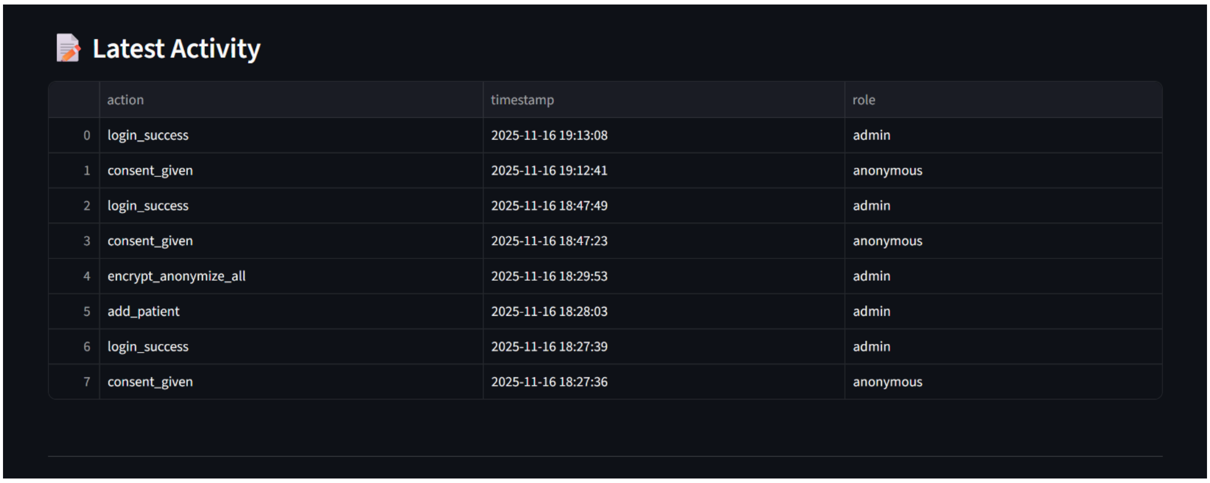
3.4 Graphs & Trends

- Visual representation of system activity and patient trends.
  - Patients per day (line chart)
  - Most common system actions (bar chart)
  - Role-based activity distribution
- Supports quick insights for admins.

Screenshot:







📝 Latest Activity

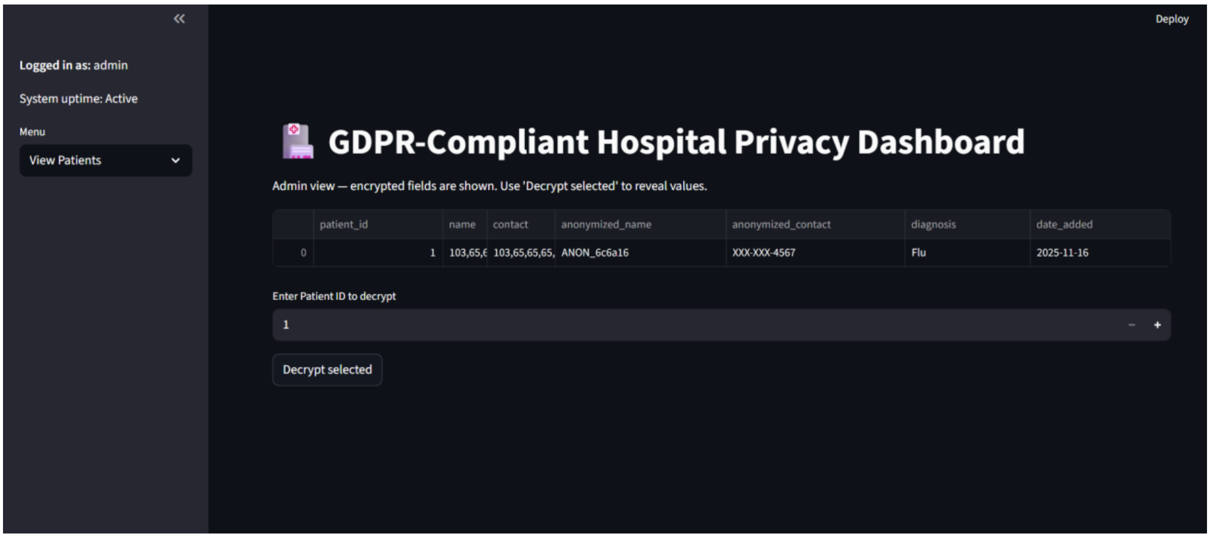
	action	timestamp	role
0	login_success	2025-11-16 19:13:08	admin
1	consent_given	2025-11-16 19:12:41	anonymous
2	login_success	2025-11-16 18:47:49	admin
3	consent_given	2025-11-16 18:47:23	anonymous
4	encrypt_anonymize_all	2025-11-16 18:29:53	admin
5	add_patient	2025-11-16 18:28:03	admin
6	login_success	2025-11-16 18:27:39	admin
7	consent_given	2025-11-16 18:27:36	anonymous

3.5 View Patients

- Display of patient records, filtered by user role:

  - Doctor: anonymized data
  - Receptionist: limited info
  - Admin: full encrypted view
- Admin can decrypt individual records as needed.

Screenshot:



Logged in as: admin

System uptime: Active

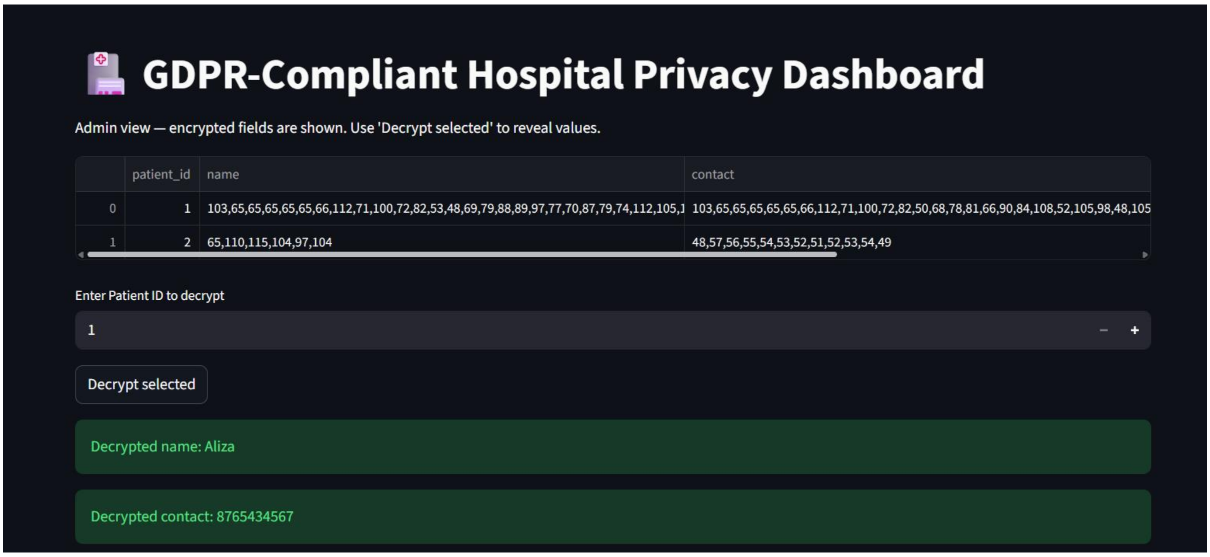
GDPR-Compliant Hospital Privacy Dashboard

Admin view — encrypted fields are shown. Use 'Decrypt selected' to reveal values.

	patient_id	name	contact	anonymized_name	anonymized_contact	diagnosis	date_added
0	1	103,65,6	103,65,65,65,	ANON_6c6a16	XXX-XXX-4567	Flu	2025-11-16

Enter Patient ID to decrypt

1



GDPR-Compliant Hospital Privacy Dashboard

Admin view — encrypted fields are shown. Use 'Decrypt selected' to reveal values.

	patient_id	name	contact
0	1	103,65,65,65,65,65,66,112,71,100,72,82,53,48,69,79,88,89,97,77,70,87,79,74,112,105,1	103,65,65,65,65,65,66,112,71,100,72,82,50,68,78,81,66,90,84,108,52,105,98,48,105
1	2	65,110,115,104,97,104	48,57,56,55,54,53,52,51,52,53,54,49

Enter Patient ID to decrypt

1

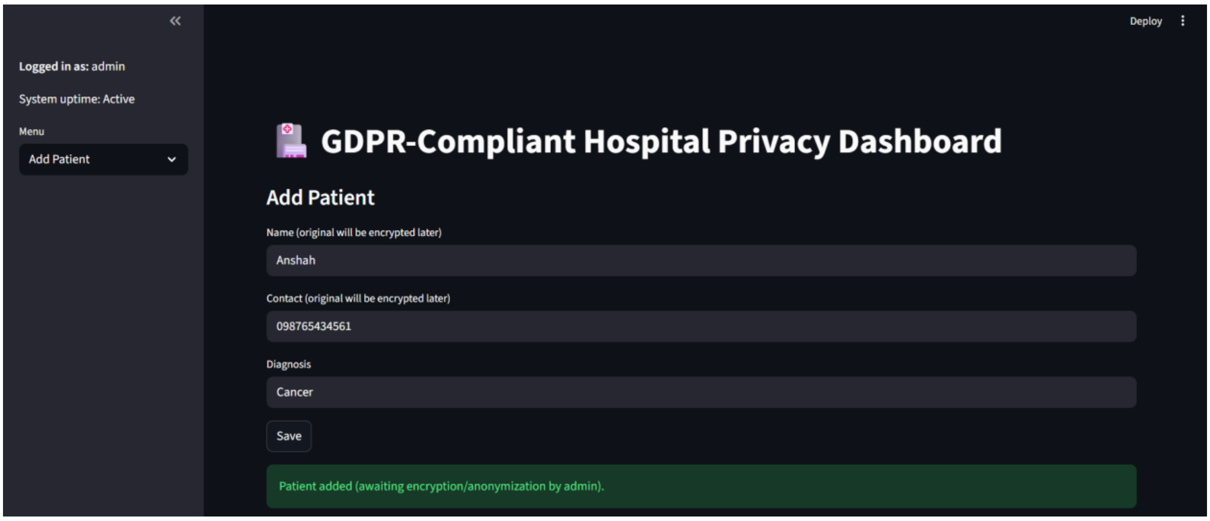
Decrypted name: Aliza

Decrypted contact: 8765434567

3.6 Add Patient

- Admins and receptionists can add new patients.
- Original name and contact encrypted later by admin.
- Audit log entry created for every addition.

Screenshot:



Logged in as: admin

System uptime: Active

Menu: Add Patient

GDPR-Compliant Hospital Privacy Dashboard

Add Patient

Name (original will be encrypted later): Anshah

Contact (original will be encrypted later): 098765434561

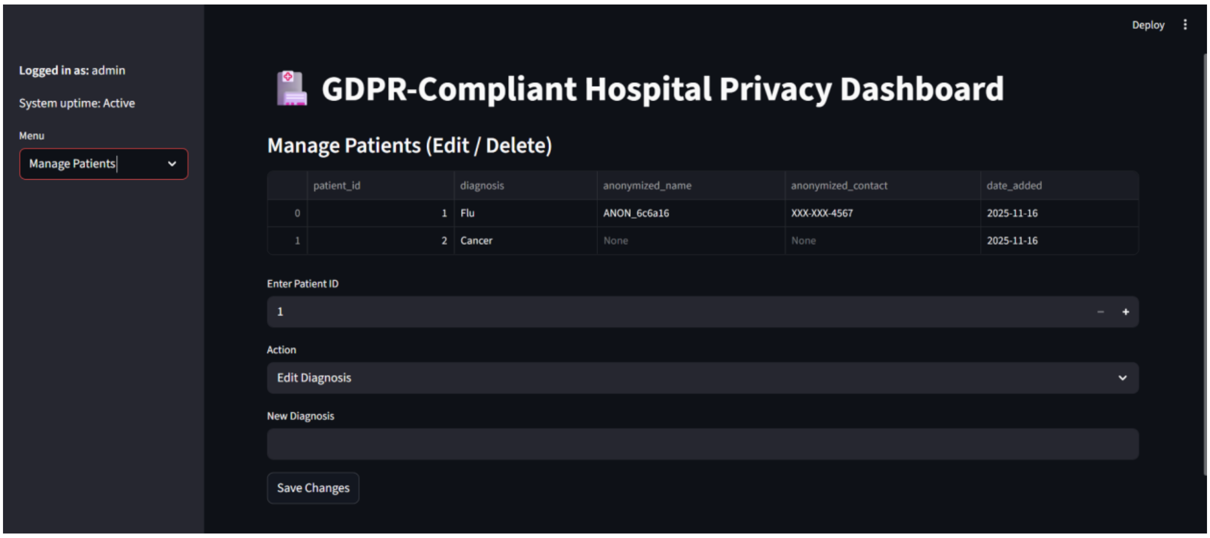
Diagnosis: Cancer

Patient added (awaiting encryption/anonymization by admin).

3.7 Manage Patients

- Edit or delete existing patient records.
- Role-based restrictions:
  - Admin: Edit diagnosis, delete patient
  - Receptionist: Edit diagnosis only
- Actions are logged for auditing.

Screenshot:



Logged in as: admin

System uptime: Active

Menu: Manage Patients

GDPR-Compliant Hospital Privacy Dashboard

Manage Patients (Edit / Delete)

	patient_id	diagnosis	anonymized_name	anonymized_contact	date_added
0	1	Flu	ANON_6c6a16	XXX-XXX-4567	2025-11-16
1	2	Cancer	None	None	2025-11-16

Enter Patient ID: 1

Action: Edit Diagnosis

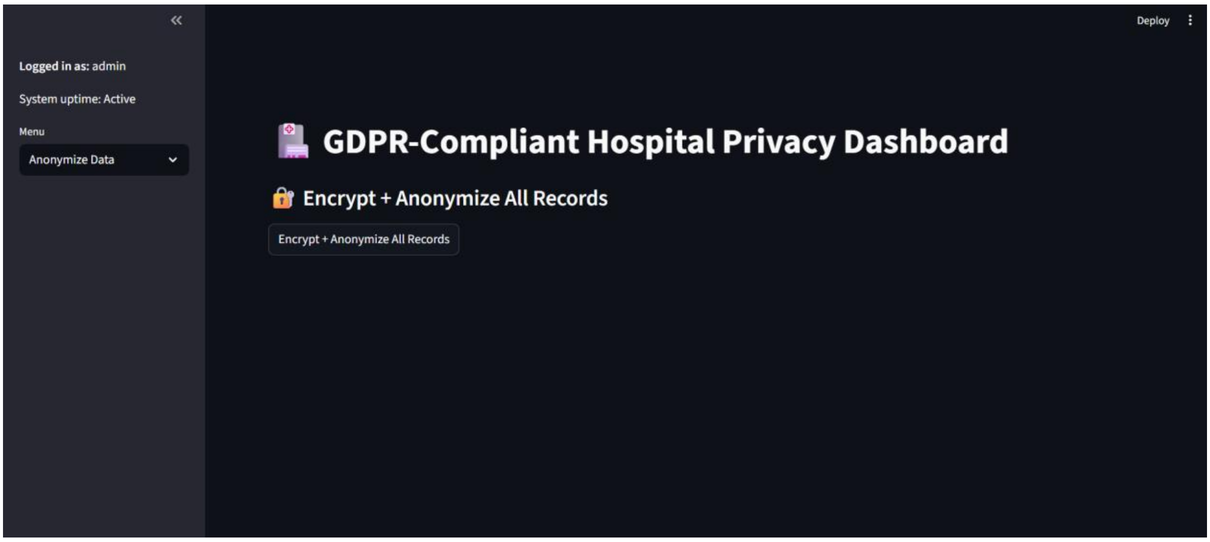
New Diagnosis:

3.8 Anonymize Data

- Admins can encrypt and anonymize all patient data in one action.
- Generates anonymized columns for safe viewing by non-admin roles.

- Creates audit log entries for compliance.

Screenshot:



Logged in as: admin

System uptime: Active

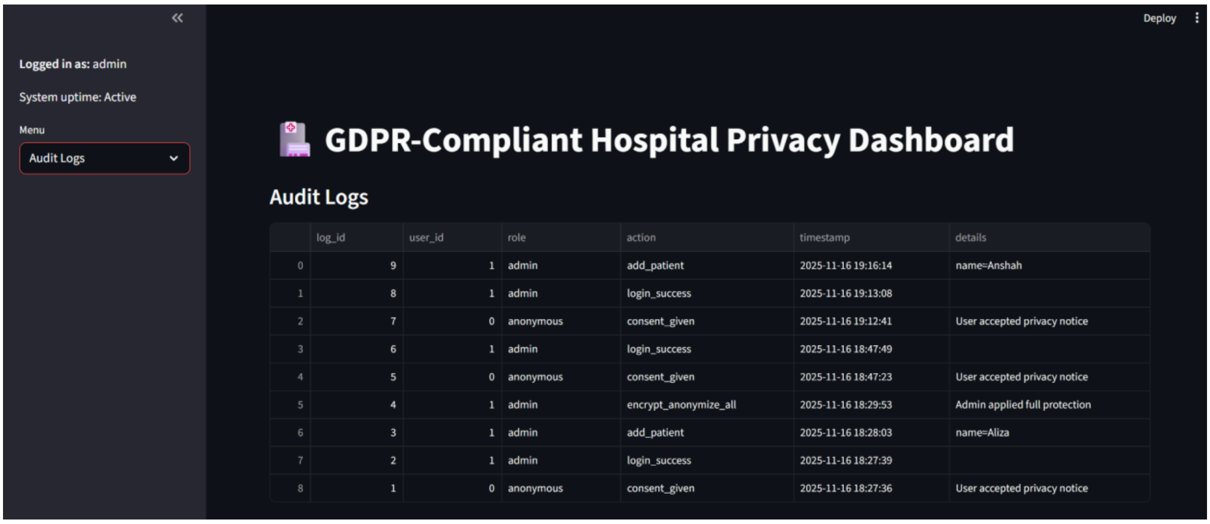
GDPR-Compliant Hospital Privacy Dashboard

🔐 Encrypt + Anonymize All Records

3.9 Audit Logs

- Shows all user actions with timestamp and role.
- Visualizations include:
  - Line chart (actions per day)
  - Bar chart (most common actions, role activity)
- Supports monitoring and auditing.

Screenshot:



Logged in as: admin

System uptime: Active

GDPR-Compliant Hospital Privacy Dashboard

Audit Logs

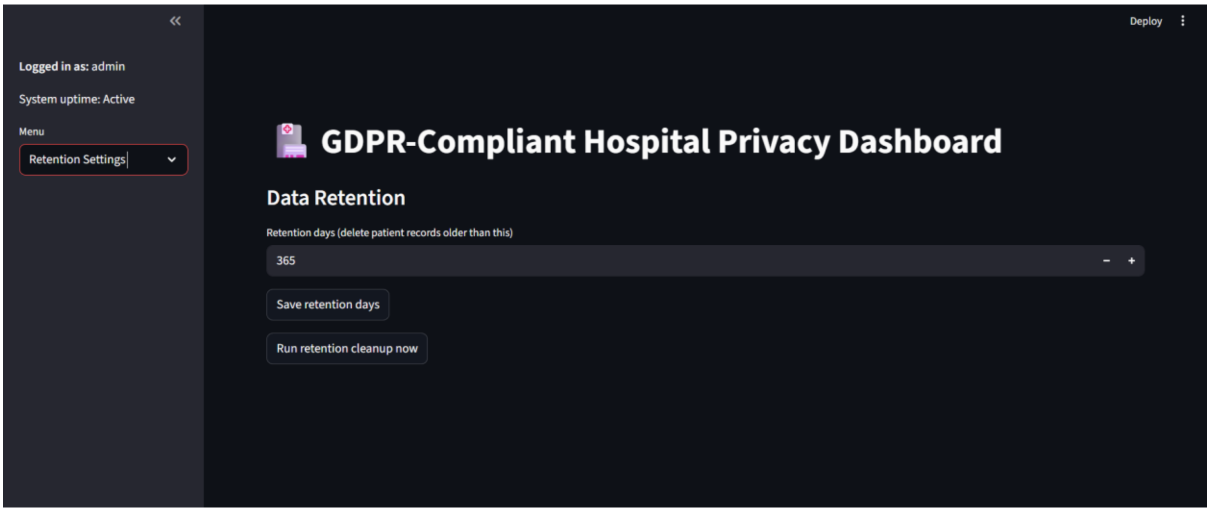
	log_id	user_id	role	action	timestamp	details
0	9	1	admin	add_patient	2025-11-16 19:16:14	name=Anshah
1	8	1	admin	login_success	2025-11-16 19:13:08	
2	7	0	anonymous	consent_given	2025-11-16 19:12:41	User accepted privacy notice
3	6	1	admin	login_success	2025-11-16 18:47:49	
4	5	0	anonymous	consent_given	2025-11-16 18:47:23	User accepted privacy notice
5	4	1	admin	encrypt_anonymize_all	2025-11-16 18:29:53	Admin applied full protection
6	3	1	admin	add_patient	2025-11-16 18:28:03	name=Aliza
7	2	1	admin	login_success	2025-11-16 18:27:39	
8	1	0	anonymous	consent_given	2025-11-16 18:27:36	User accepted privacy notice

---

3.10 Retention Settings

- Configure number of days to retain patient records.
- Run retention cleanup to remove old records.
- Logs all retention actions for audit purposes.

Screenshot:



Logged in as: admin

System uptime: Active

Menu: Retention Settings

GDPR-Compliant Hospital Privacy Dashboard

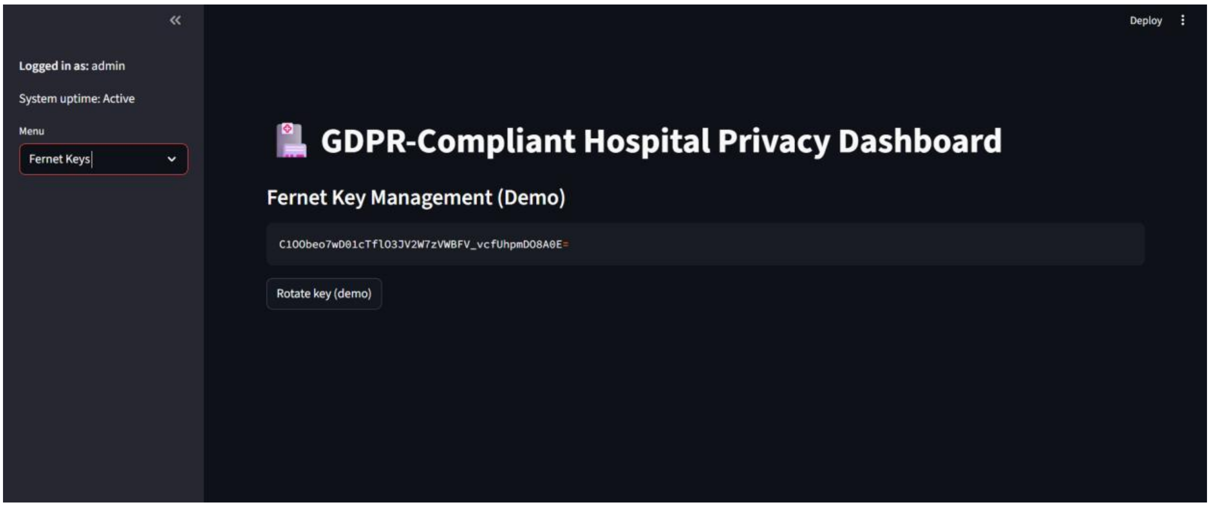
Data Retention

Retention days (delete patient records older than this): 365

3.11 Fernet Keys

- Display current encryption key (demo purposes only)
- Rotate key safely while keeping existing records decryptable.
- Ensures confidentiality layer in CIA.

Screenshot:



Logged in as: admin

System uptime: Active

Menu: Fernet Keys

GDPR-Compliant Hospital Privacy Dashboard

Fernet Key Management (Demo)

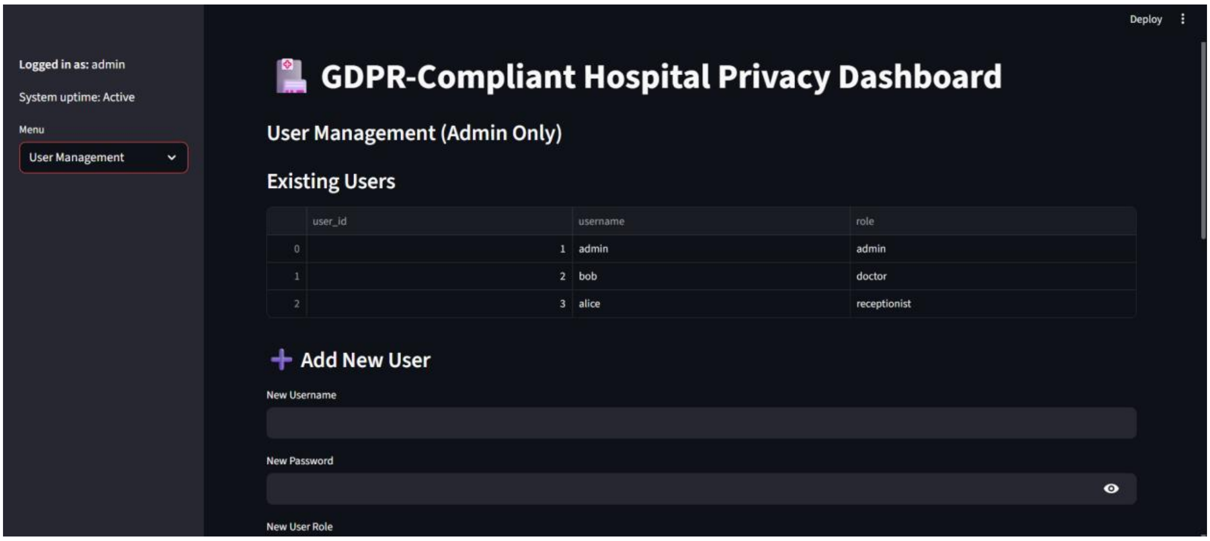
```
C1OObeo7wD01cTflO3JV2W7zVWBFV_vcfUhpmDO8A0E=
```

3.12 User Management

- Admins can add, edit, or delete users.

- Role assignment for doctors, receptionists, or admins.
- Actions logged for audit trail.

Screenshot:



GDPR-Compliant Hospital Privacy Dashboard

User Management (Admin Only)

Existing Users

	user_id	username	role
0	1	admin	admin
1	2	bob	doctor
2	3	alice	receptionist

➕ Add New User

New Username

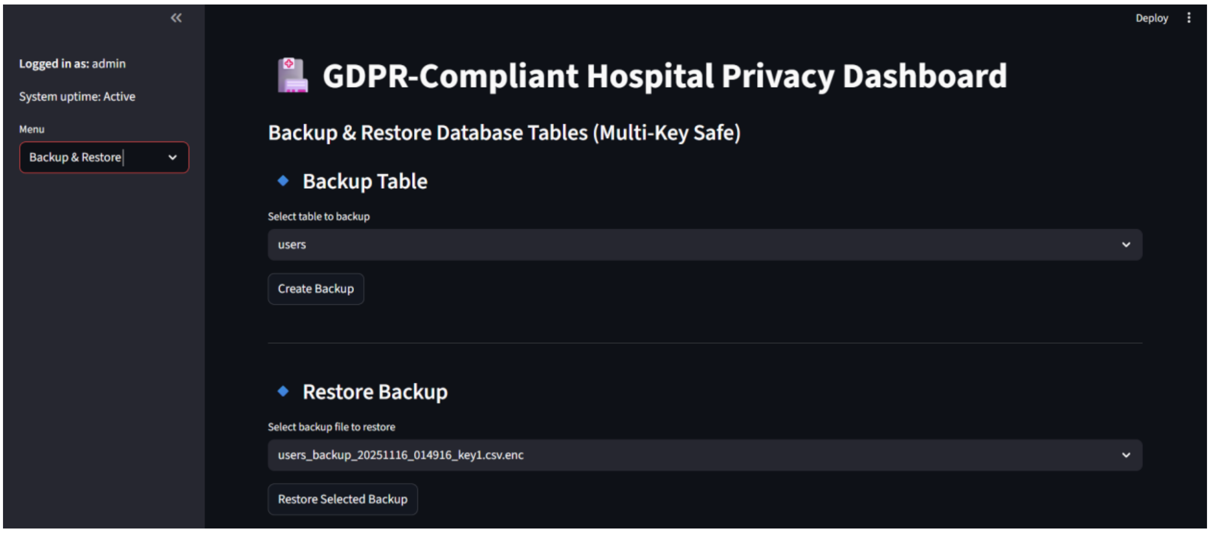
New Password

New User Role

3.13 Backup & Restore

- Backup selected tables to encrypted files.
- Restore backups while respecting key versioning.
- Ensures availability and disaster recovery.

Screenshot:



GDPR-Compliant Hospital Privacy Dashboard

Backup & Restore Database Tables (Multi-Key Safe)

🔹 Backup Table

Select table to backup: users

🔹 Restore Backup

Select backup file to restore: users_backup_20251116_014916_key1.csv.enc

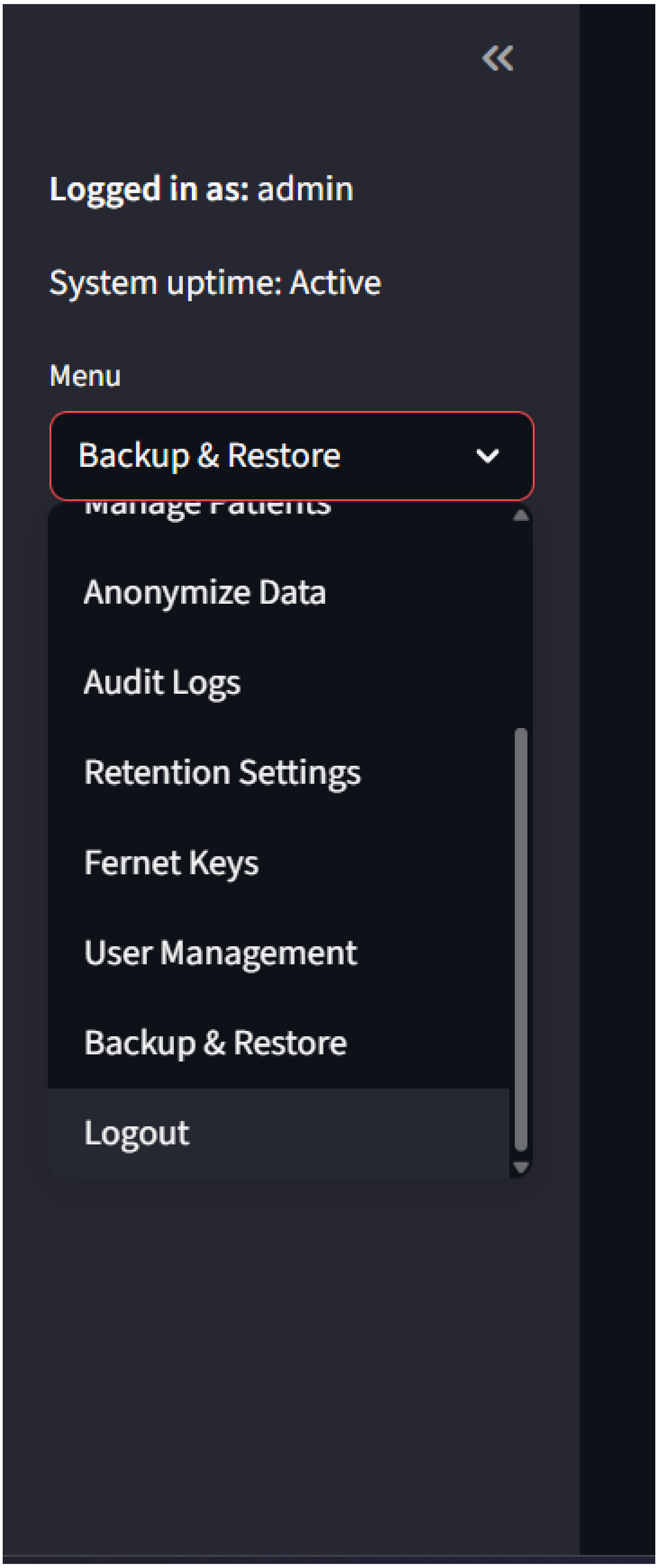
---

3.14 Logout

- Ends session and logs out user.

- Ensures session security.

Screenshot:

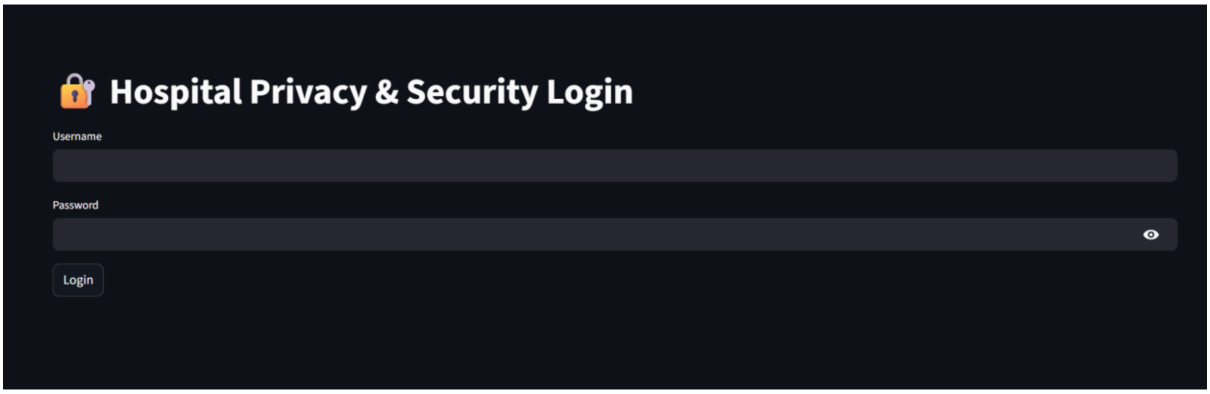


Logged in as: admin

System uptime: Active

Menu

Backup & Restore



4. Discussion: CIA Principles & GDPR Alignment

4.1 Confidentiality

- Encrypted storage of patient names and contact details ensures only authorized personnel (admins) can decrypt.
- Anonymization prevents disclosure to doctors and receptionists beyond necessity.

4.2 Integrity

- All system actions logged to logs table.
- Re-encryption operations preserve data correctness even after key rotations.

4.3 Availability

- Regular backups and key-safe restore processes maintain data availability.
- System uptime monitoring ensures operational reliability.

4.4 GDPR Compliance

- **Consent:** Users must consent to data processing before login.
- **Minimization & Pseudonymization:** Anonymized names and contacts limit exposure.
- **Retention:** Configurable retention policies automatically remove old records.
- **Auditability:** All actions are traceable for accountability.

5. Conclusion

The Hospital Privacy Dashboard effectively combines **security best practices** with **GDPR principles**:

- **Data security:** Encryption + anonymization
- **Auditability:** Comprehensive logs and visualization
- **Controlled access:** Role-based permissions
- **Operational reliability:** Uptime monitoring & backups
- **GDPR alignment:** Consent, retention, pseudonymization

This system demonstrates a practical approach to **secure healthcare data management** in compliance with modern regulations.

Video Link: https://drive.google.com/file/d/1EyLom01NETlBCQ9VuIqYmRxt7QBmK-NY/view?usp=sharing