Information Security
Assignment 4

22K-4413

BCS-7H

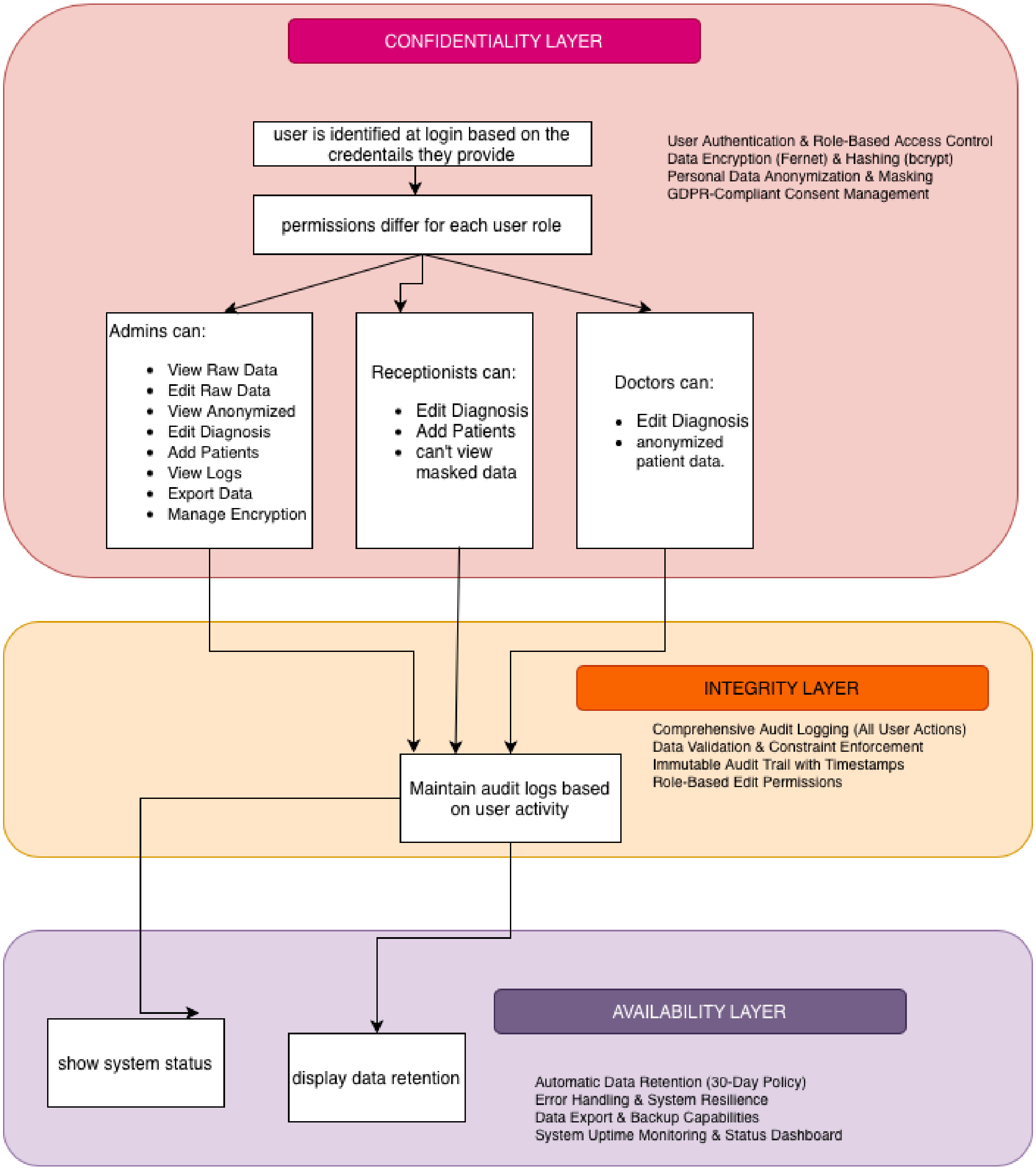
Instructor: Dr Aqsa Aslam

TABLE OF CONTENT

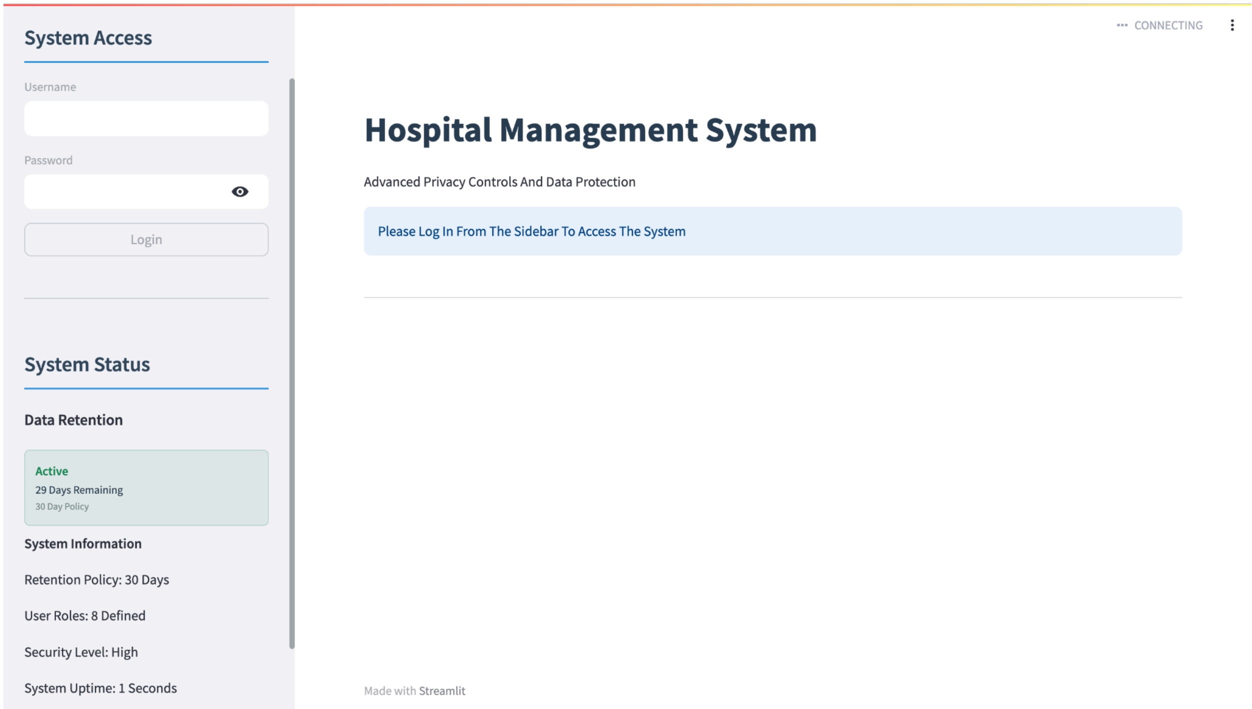
https://github.com/SyedaFakhiraSaghir/Hospital-Management-System-Implementing-CIA-triad/blob/main/main.py

SYSTEM OVERVIEW DIAGRAM

Drawn on draw.io: link to diagram


CONFIDENTIALITY LAYER
user is identified at login based on the credentails they provide
permissions differ for each user role
User Authentication & Role-Based Access Control
Data Encryption (Fernet) & Hashing (bcrypt)
Personal Data Anonymization & Masking
GDPR-Compliant Consent Management
Admins can:
View Raw Data
Edit Raw Data
View Anonymized
Edit Diagnosis
Add Patients
View Logs
Export Data
Manage Encryption
Receptionists can:
Edit Diagnosis
Add Patients
can't view masked data
Doctors can:
Edit Diagnosis
anonymized patient data.
INTEGRITY LAYER
Comprehensive Audit Logging (All User Actions)
Data Validation & Constraint Enforcement
Immutable Audit Trail with Timestamps
Role-Based Edit Permissions
Maintain audit logs based on user activity
AVAILABILITY LAYER
show system status
display data retention
Automatic Data Retention (30-Day Policy)
Error Handling & System Resilience
Data Export & Backup Capabilities
System Uptime Monitoring & Status Dashboard

SCREENSHOTS SECTION



Hospital Management System

Advanced Privacy Controls And Data Protection

Please Log In From The Sidebar To Access The System

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

System Uptime: 1 Seconds

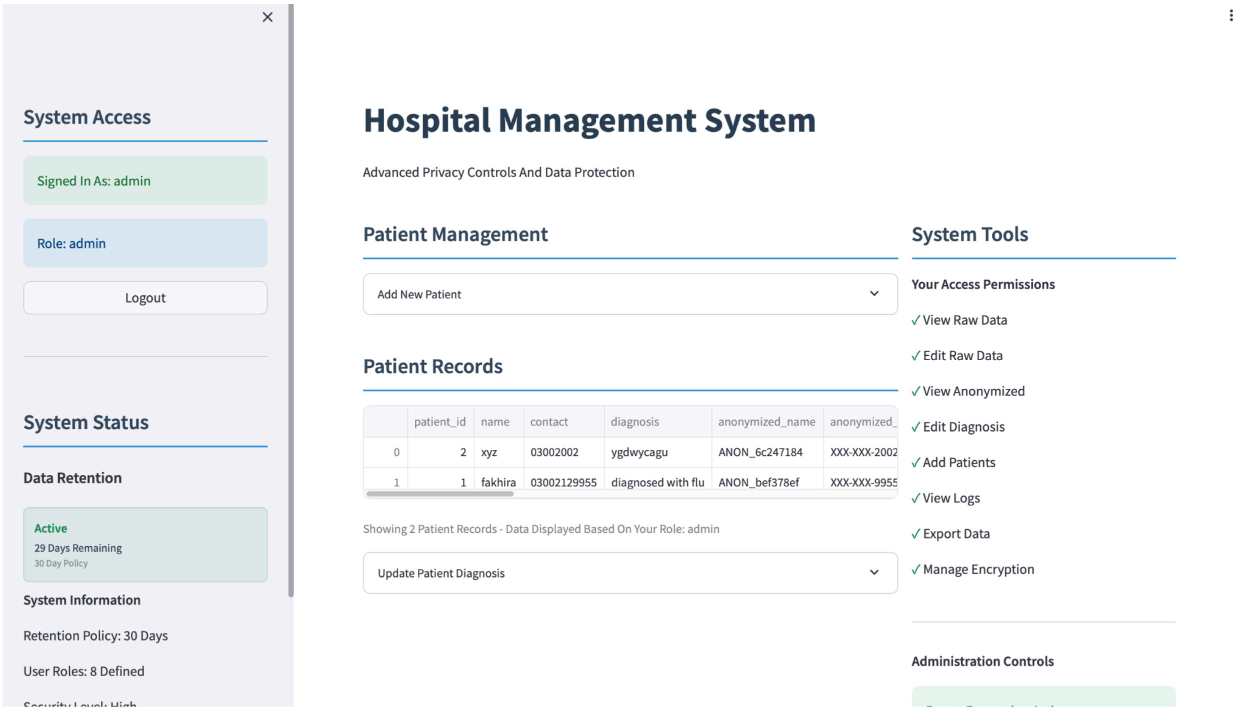
Login Page:

- Secure authentication with role-based access
- System Status displayed

Features:

- Username/password fields
- Error handling
- Session management and display of data retention

ROLE: ADMIN



System Access

Signed In As: admin

Role: admin

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Hospital Management System

Advanced Privacy Controls And Data Protection

Patient Management

Patient Records

	patient_id	name	contact	diagnosis	anonymized_name	anonymized_
0	2	xyz	03002002	ygdwycagu	ANON_6c247184	XXX-XXX-2002
1	1	fakhira	03002129955	diagnosed with flu	ANON_bef378ef	XXX-XXX-9955

Showing 2 Patient Records - Data Displayed Based On Your Role: admin

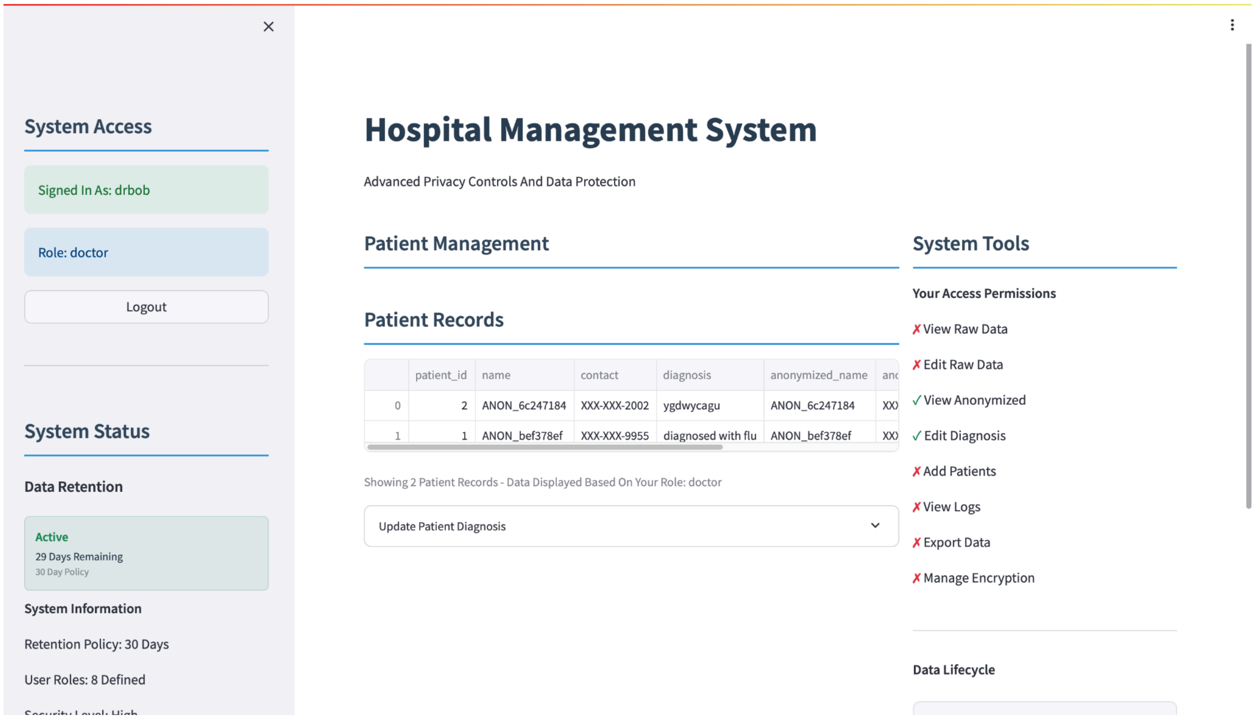
System Tools

Your Access Permissions

✓ View Raw Data
✓ Edit Raw Data
✓ View Anonymized
✓ Edit Diagnosis
✓ Add Patients
✓ View Logs
✓ Export Data
✓ Manage Encryption

Administration Controls

ROLE: DOCTOR



System Access

Signed In As: drbob

Role: doctor

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Hospital Management System

Advanced Privacy Controls And Data Protection

Patient Management

Patient Records

	patient_id	name	contact	diagnosis	anonymized_name	anc
0	2	ANON_6c247184	XXX-XXX-2002	ygdwycagu	ANON_6c247184	XX)
1	1	ANON_bef378ef	XXX-XXX-9955	diagnosed with flu	ANON_bef378ef	XX)

Showing 2 Patient Records - Data Displayed Based On Your Role: doctor

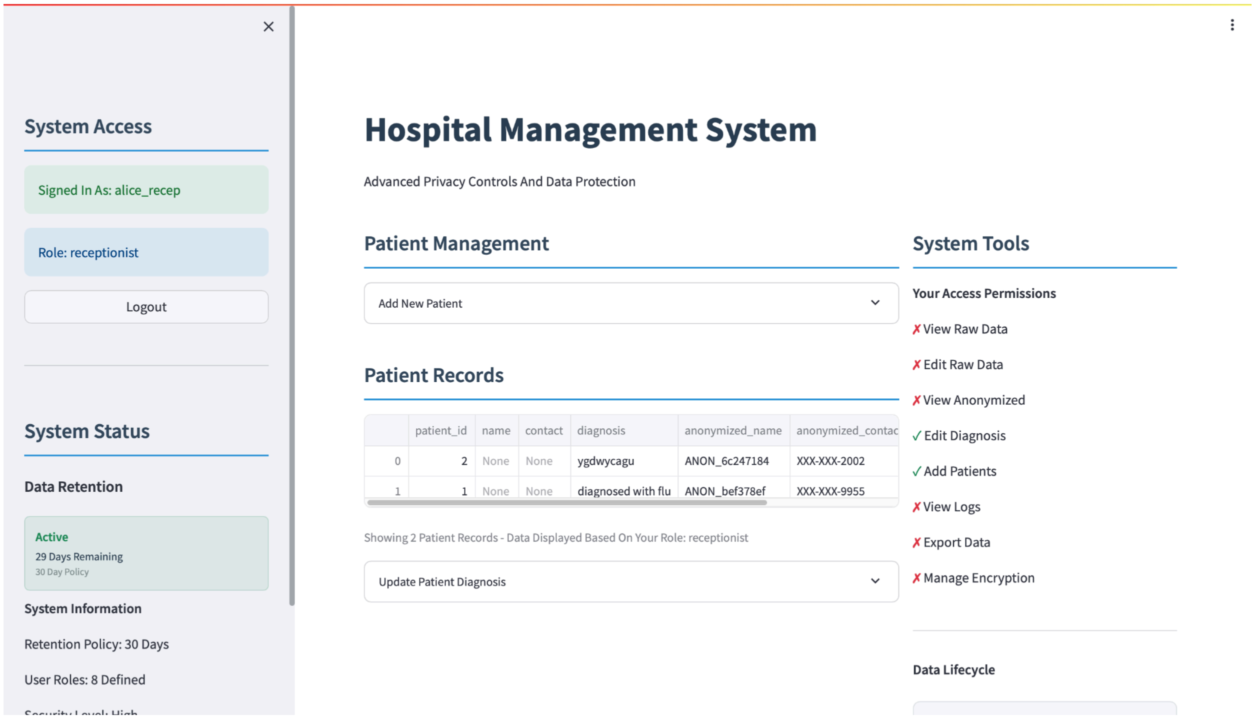
System Tools

Your Access Permissions

✗ View Raw Data
✗ Edit Raw Data
✓ View Anonymized
✓ Edit Diagnosis
✗ Add Patients
✗ View Logs
✗ Export Data
✗ Manage Encryption

Data Lifecycle

ROLE: RECEPTIONIST



System Access

Signed In As: alice_recep

Role: receptionist

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Hospital Management System

Advanced Privacy Controls And Data Protection

Patient Management

Patient Records

	patient_id	name	contact	diagnosis	anonymized_name	anonymized_contac
0	2	None	None	ygdwycagu	ANON_6c247184	XXX-XXX-2002
1	1	None	None	diagnosed with flu	ANON_bef378ef	XXX-XXX-9955

Showing 2 Patient Records - Data Displayed Based On Your Role: receptionist

System Tools

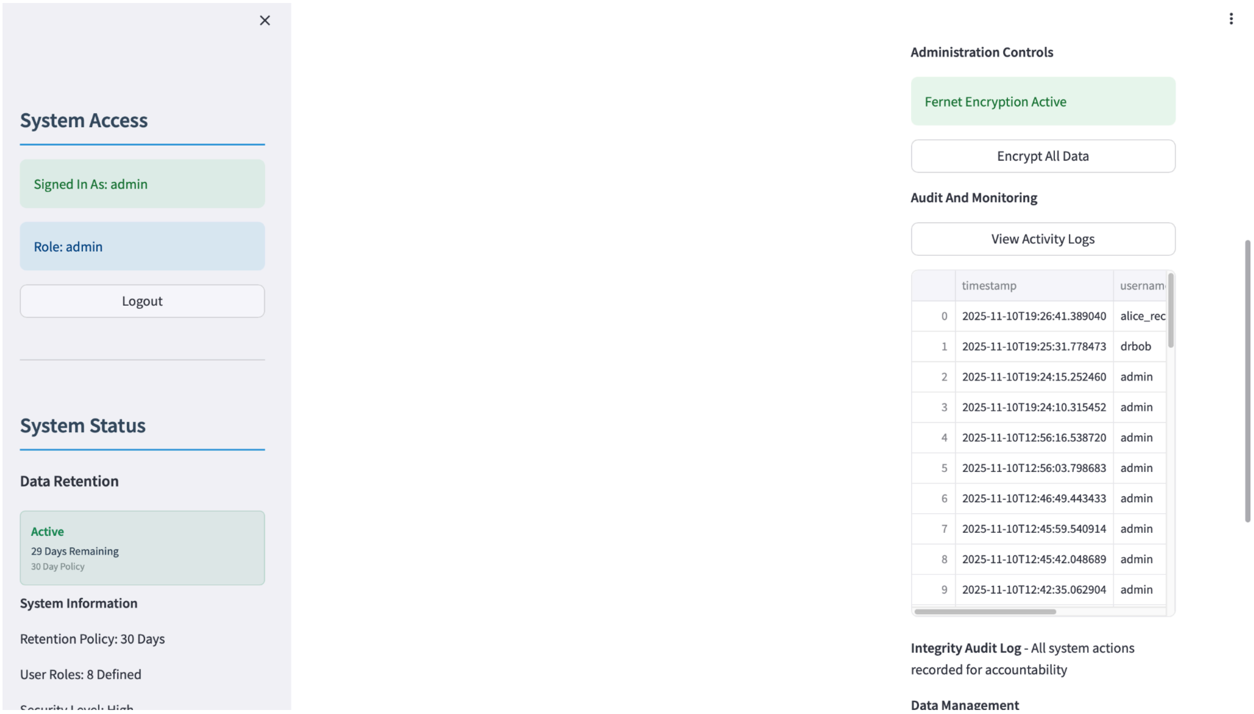
Your Access Permissions

✗ View Raw Data
✗ Edit Raw Data
✗ View Anonymized
✓ Edit Diagnosis
✓ Add Patients
✗ View Logs
✗ Export Data
✗ Manage Encryption

Data Lifecycle

- Real-time anonymization (ANON_8a3d, XXX-XXX-1234)
- Different data visibility for doctor, admin and receptionist
- Automatic masking and encryption

Activity Logs



System Access

Signed In As: admin

Role: admin

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Administration Controls

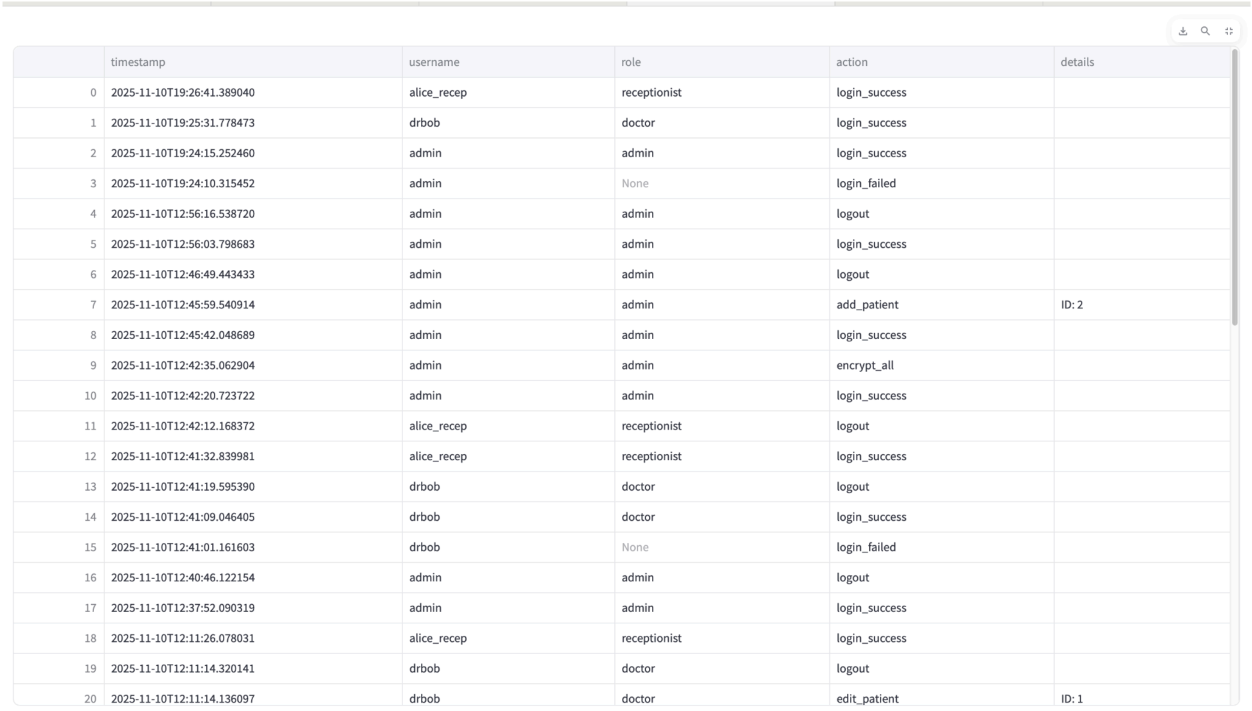
Fernet Encryption Active

Audit And Monitoring

	timestamp	usernam
0	2025-11-10T19:26:41.389040	alice_rec
1	2025-11-10T19:25:31.778473	drbob
2	2025-11-10T19:24:15.252460	admin
3	2025-11-10T19:24:10.315452	admin
4	2025-11-10T12:56:16.538720	admin
5	2025-11-10T12:56:03.798683	admin
6	2025-11-10T12:46:49.443433	admin
7	2025-11-10T12:45:59.540914	admin
8	2025-11-10T12:45:42.048689	admin
9	2025-11-10T12:42:35.062904	admin

Integrity Audit Log - All system actions recorded for accountability

Data Management

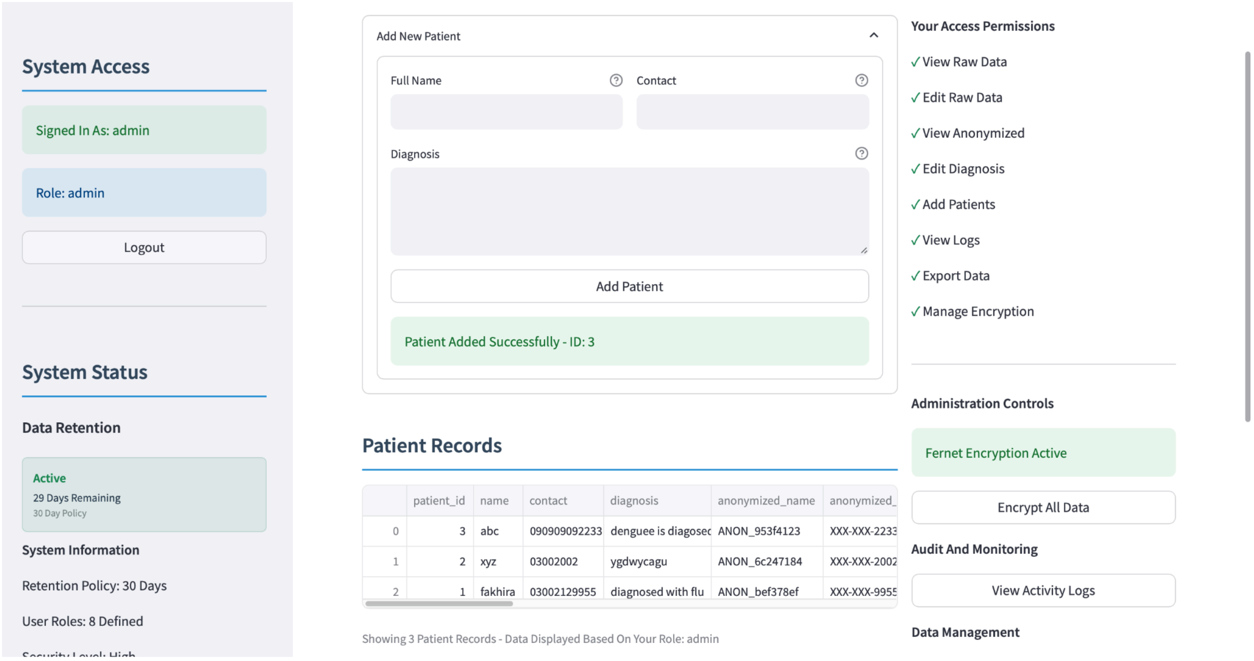


	timestamp	username	role	action	details
0	2025-11-10T19:26:41.389040	alice_recep	receptionist	login_success	
1	2025-11-10T19:25:31.778473	drbob	doctor	login_success	
2	2025-11-10T19:24:15.252460	admin	admin	login_success	
3	2025-11-10T19:24:10.315452	admin	None	login_failed	
4	2025-11-10T12:56:16.538720	admin	admin	logout	
5	2025-11-10T12:56:03.798683	admin	admin	login_success	
6	2025-11-10T12:46:49.443433	admin	admin	logout	
7	2025-11-10T12:45:59.540914	admin	admin	add_patient	ID: 2
8	2025-11-10T12:45:42.048689	admin	admin	login_success	
9	2025-11-10T12:42:35.062904	admin	admin	encrypt_all	
10	2025-11-10T12:42:20.723722	admin	admin	login_success	
11	2025-11-10T12:42:12.168372	alice_recep	receptionist	logout	
12	2025-11-10T12:41:32.839981	alice_recep	receptionist	login_success	
13	2025-11-10T12:41:19.595390	drbob	doctor	logout	
14	2025-11-10T12:41:09.046405	drbob	doctor	login_success	
15	2025-11-10T12:41:01.161603	drbob	None	login_failed	
16	2025-11-10T12:40:46.122154	admin	admin	logout	
17	2025-11-10T12:37:52.090319	admin	admin	login_success	
18	2025-11-10T12:11:26.078031	alice_recep	receptionist	login_success	
19	2025-11-10T12:11:14.320141	drbob	doctor	logout	
20	2025-11-10T12:11:14.136097	drbob	doctor	edit_patient	ID: 1

- Action logging maintains integrity
- Timestamped records of all system activities help keep audit trail
- Exclusive log viewing for admin only

ADDED PATIENTS USING ADMIN

Fernet encryption can be seen for reversible anonymization.



System Access

Signed In As: admin

Role: admin

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Add New Patient

Full Name

Contact

Diagnosis

Patient Added Successfully - ID: 3

Patient Records

	patient_id	name	contact	diagnosis	anonymized_name	anonymized_
0	3	abc	090909092233	denguee is diagosec	ANON_953f4123	XXX-XXX-2233
1	2	xyz	03002002	ygdwycagu	ANON_6c247184	XXX-XXX-2002
2	1	fakhira	03002129955	diagnosed with flu	ANON_bef378ef	XXX-XXX-9955

Showing 3 Patient Records - Data Displayed Based On Your Role: admin

Your Access Permissions

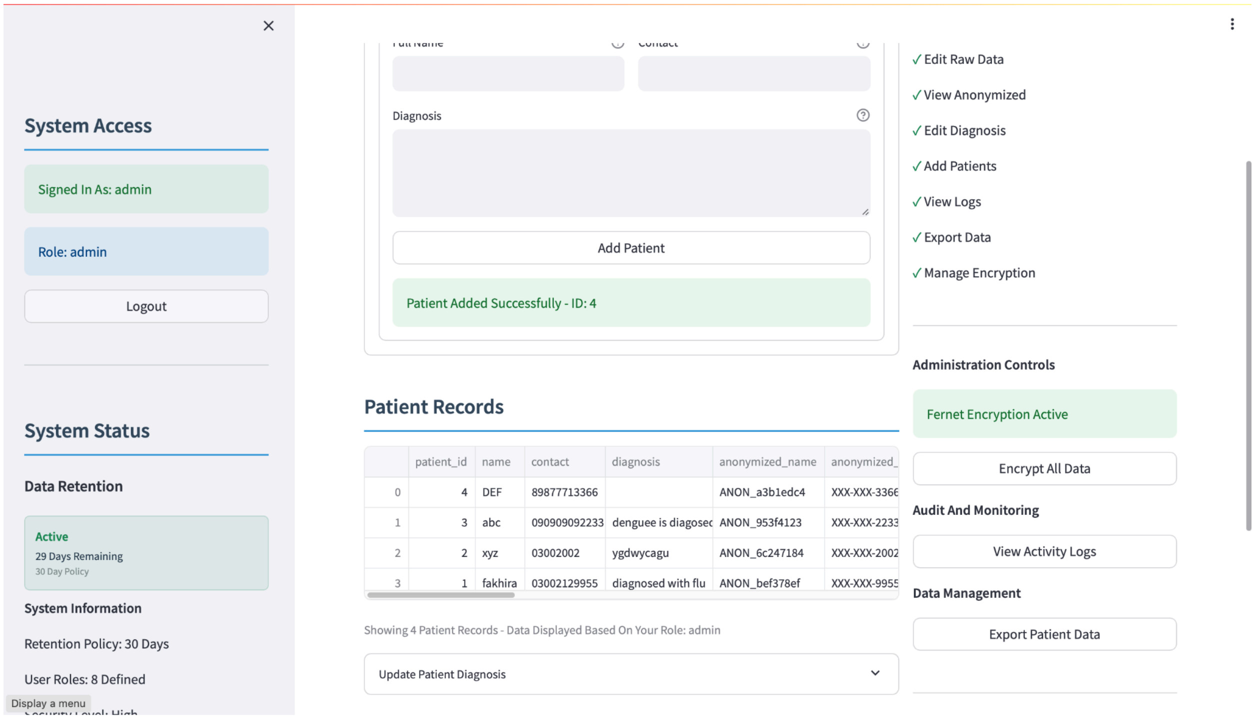
✓ View Raw Data
✓ Edit Raw Data
✓ View Anonymized
✓ Edit Diagnosis
✓ Add Patients
✓ View Logs
✓ Export Data
✓ Manage Encryption

Administration Controls

Fernet Encryption Active

Audit And Monitoring

Data Management



System Access

Signed In As: admin

Role: admin

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Full Name

Contact

Diagnosis

Patient Added Successfully - ID: 4

Patient Records

	patient_id	name	contact	diagnosis	anonymized_name	anonymized_
0	4	DEF	89877713366		ANON_a3b1edc4	XXX-XXX-3366
1	3	abc	090909092233	denguee is diagosec	ANON_953f4123	XXX-XXX-2233
2	2	xyz	03002002	ygdwycagu	ANON_6c247184	XXX-XXX-2002
3	1	fakhira	03002129955	diagnosed with flu	ANON_bef378ef	XXX-XXX-9955

Showing 4 Patient Records - Data Displayed Based On Your Role: admin

Update Patient Diagnosis

✓ Edit Raw Data
✓ View Anonymized
✓ Edit Diagnosis
✓ Add Patients
✓ View Logs
✓ Export Data
✓ Manage Encryption

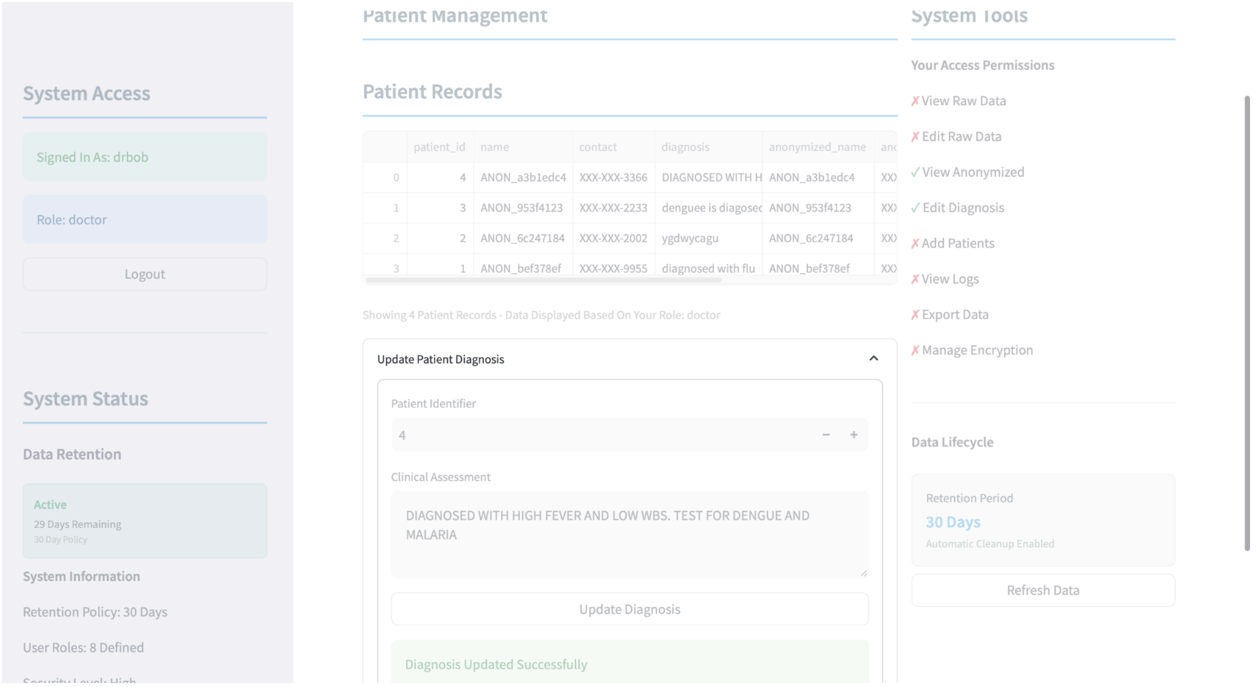
Administration Controls

Fernet Encryption Active

Audit And Monitoring

Data Management

DOCTOR UPDATES THE DIAGNOSIS:



System Access

Signed In As: drbob

Role: doctor

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Patient Records

	patient_id	name	contact	diagnosis	anonymized_name	anc
0	4	ANON_a3b1edc4	XXX-XXX-3366	DIAGNOSED WITH H	ANON_a3b1edc4	XX)
1	3	ANON_953f4123	XXX-XXX-2233	denguee is diagosec	ANON_953f4123	XX)
2	2	ANON_6c247184	XXX-XXX-2002	ygdwycagu	ANON_6c247184	XX)
3	1	ANON_bef378ef	XXX-XXX-9955	diagnosed with flu	ANON_bef378ef	XX)

Showing 4 Patient Records - Data Displayed Based On Your Role: doctor

Update Patient Diagnosis

Patient Identifier: 4

Clinical Assessment: DIAGNOSED WITH HIGH FEVER AND LOW WBS. TEST FOR DENGUE AND MALARIA

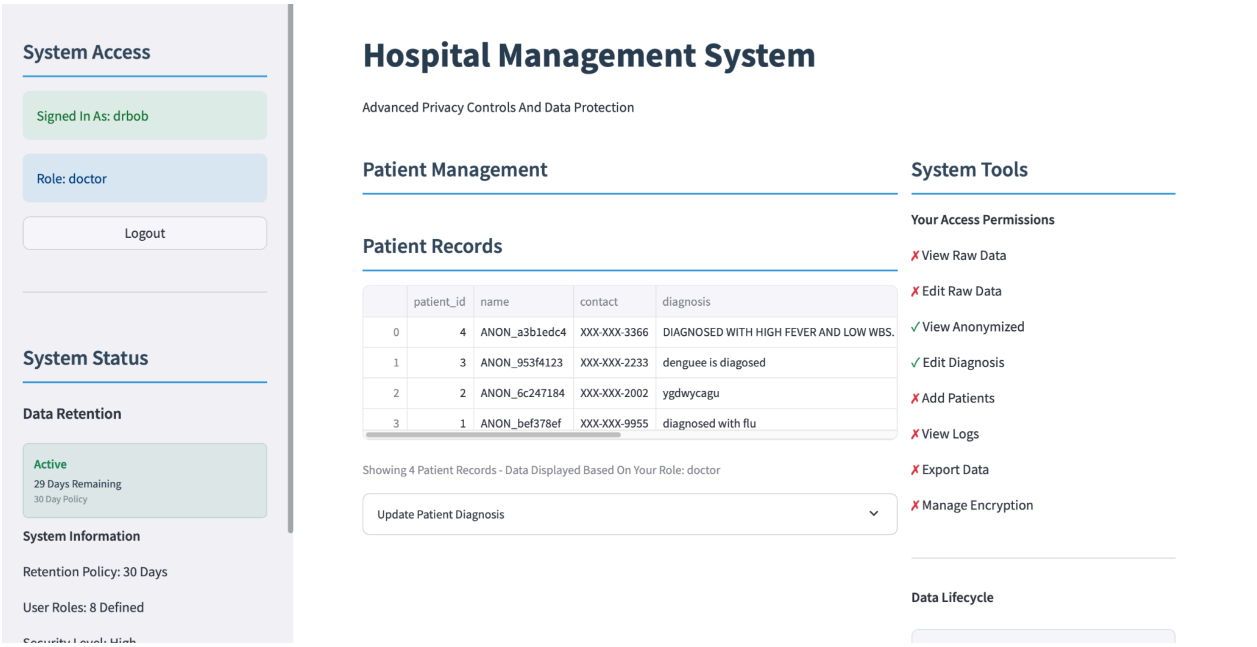
Diagnosis Updated Successfully

Your Access Permissions

✗ View Raw Data
✗ Edit Raw Data
✓ View Anonymized
✓ Edit Diagnosis
✗ Add Patients
✗ View Logs
✗ Export Data
✗ Manage Encryption

Data Lifecycle

Retention Period
30 Days
Automatic Cleanup Enabled



Hospital Management System

Advanced Privacy Controls And Data Protection

System Access

Signed In As: drbob

Role: doctor

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Patient Management

Patient Records

	patient_id	name	contact	diagnosis
0	4	ANON_a3b1edc4	XXX-XXX-3366	DIAGNOSED WITH HIGH FEVER AND LOW WBS.
1	3	ANON_953f4123	XXX-XXX-2233	denguee is diagosed
2	2	ANON_6c247184	XXX-XXX-2002	ygdwycagu
3	1	ANON_bef378ef	XXX-XXX-9955	diagnosed with flu

Showing 4 Patient Records - Data Displayed Based On Your Role: doctor

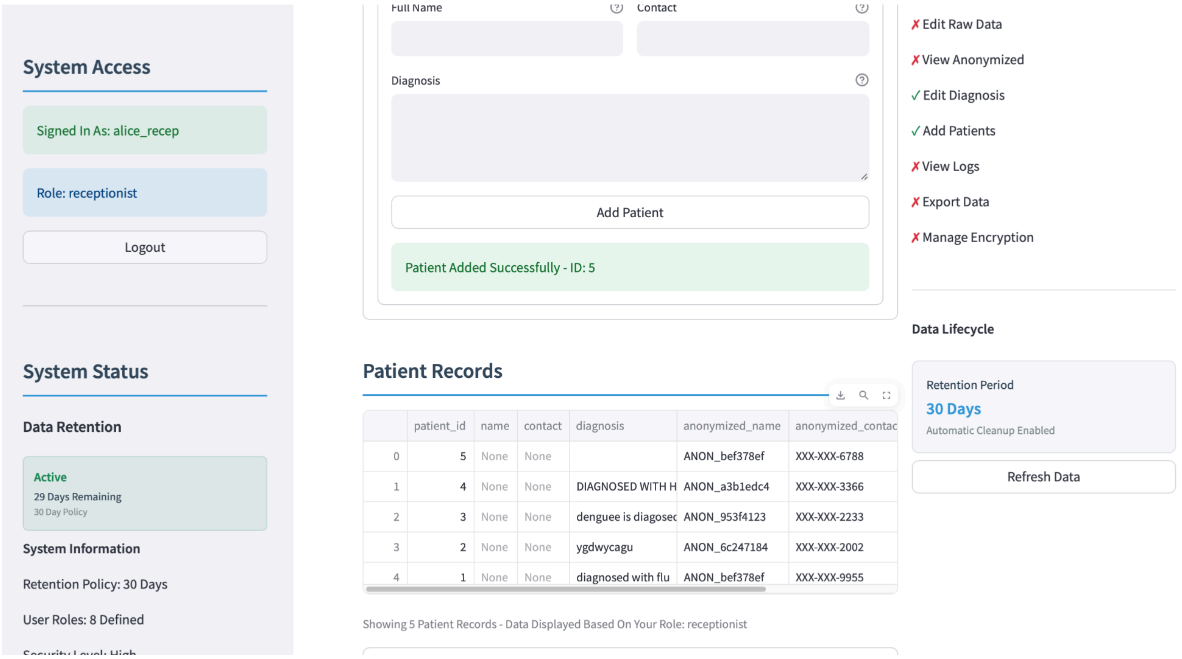
System Tools

Your Access Permissions

✗ View Raw Data
✗ Edit Raw Data
✓ View Anonymized
✓ Edit Diagnosis
✗ Add Patients
✗ View Logs
✗ Export Data
✗ Manage Encryption

Data Lifecycle

Added patient with id 5 using the receptionist panel



System Access

Signed In As: alice_recep

Role: receptionist

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

Full Name

Contact

Diagnosis

Patient Added Successfully - ID: 5

Patient Records

	patient_id	name	contact	diagnosis	anonymized_name	anonymized_contac
0	5	None	None		ANON_bef378ef	XXX-XXX-6788
1	4	None	None	DIAGNOSED WITH H	ANON_a3b1edc4	XXX-XXX-3366
2	3	None	None	denguee is diagosec	ANON_953f4123	XXX-XXX-2233
3	2	None	None	ygdwycagu	ANON_6c247184	XXX-XXX-2002
4	1	None	None	diagnosed with flu	ANON_bef378ef	XXX-XXX-9955

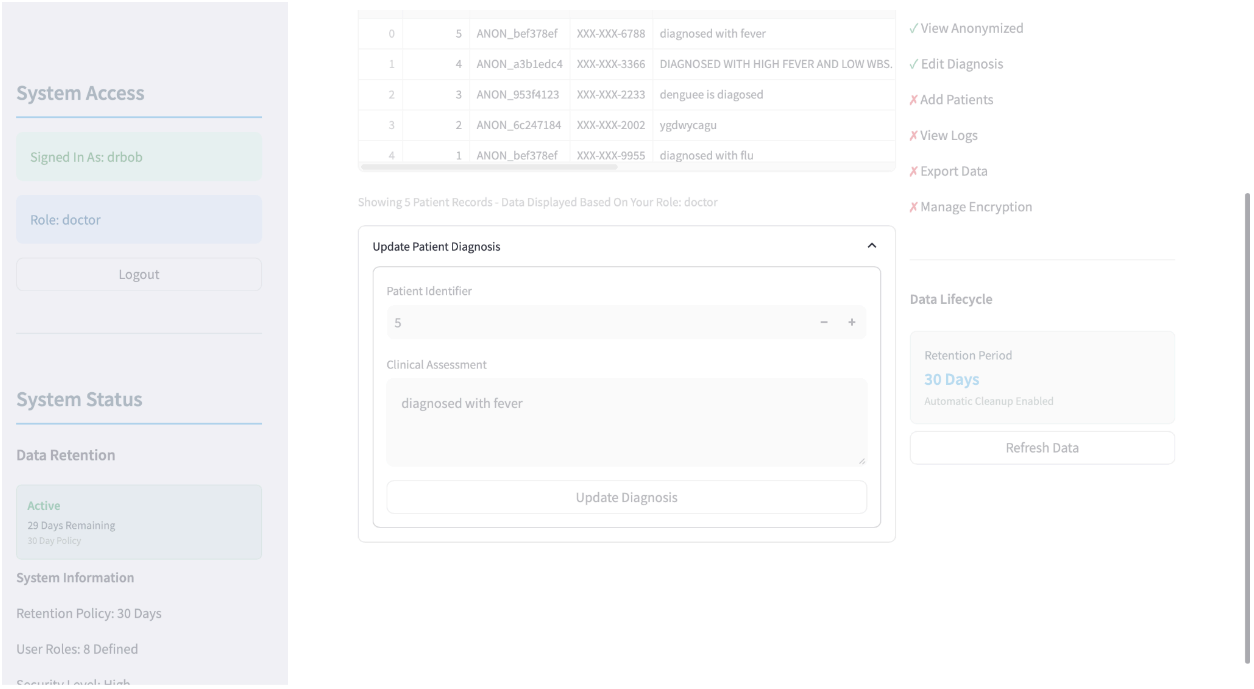
Showing 5 Patient Records - Data Displayed Based On Your Role: receptionist

✗ Edit Raw Data
✗ View Anonymized
✓ Edit Diagnosis
✓ Add Patients
✗ View Logs
✗ Export Data
✗ Manage Encryption

Data Lifecycle

Retention Period
30 Days
Automatic Cleanup Enabled

Doctor diagnosed the patient with id 5



System Access

Signed In As: drbob

Role: doctor

System Status

Data Retention

Active
29 Days Remaining
30 Day Policy

System Information

Retention Policy: 30 Days

User Roles: 8 Defined

Security Level: High

0	5	ANON_bef378ef	XXX-XXX-6788	diagnosed with fever
1	4	ANON_a3b1edc4	XXX-XXX-3366	DIAGNOSED WITH HIGH FEVER AND LOW WBS.
2	3	ANON_953f4123	XXX-XXX-2233	denguee is diagosed
3	2	ANON_6c247184	XXX-XXX-2002	ygdwycagu
4	1	ANON_bef378ef	XXX-XXX-9955	diagnosed with flu

Showing 5 Patient Records - Data Displayed Based On Your Role: doctor

Update Patient Diagnosis

Patient Identifier: 5

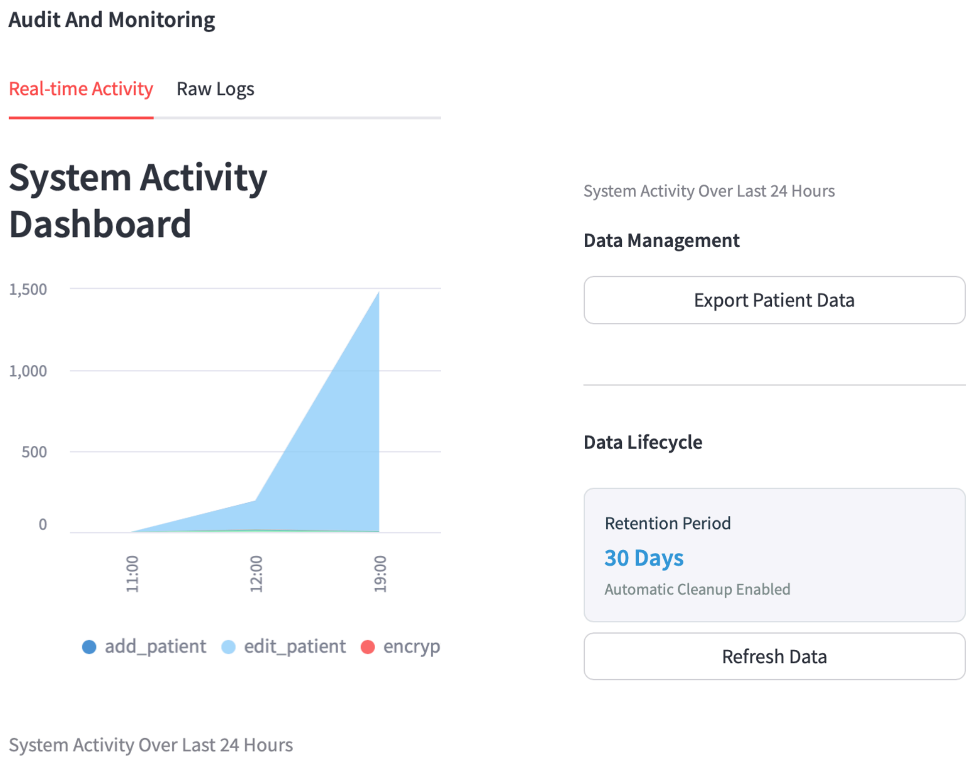
Clinical Assessment: diagnosed with fever

✓ View Anonymized
✓ Edit Diagnosis
✗ Add Patients
✗ View Logs
✗ Export Data
✗ Manage Encryption

Data Lifecycle

Retention Period
30 Days
Automatic Cleanup Enabled

Display real-time activity graphs (e.g., user actions per day).



Audit And Monitoring

Real-time Activity | Raw Logs

System Activity Dashboard

System Activity Over Last 24 Hours

System Activity Over Last 24 Hours

Data Management

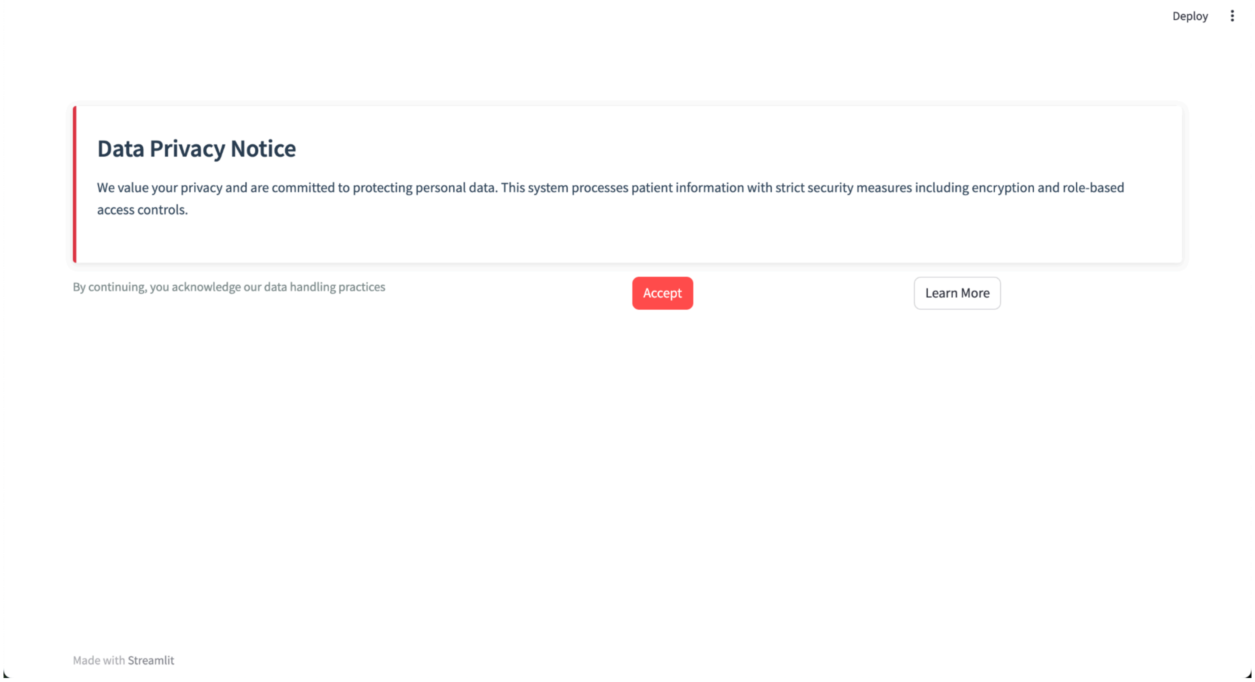
Data Lifecycle

Retention Period

30 Days

Automatic Cleanup Enabled

When the app start this user consent banner is shown:



Data Privacy Notice

We value your privacy and are committed to protecting personal data. This system processes patient information with strict security measures including encryption and role-based access controls.

By continuing, you acknowledge our data handling practices

CIA IMPLEMENTATION & GDPR ALIGNMENT

Confidentiality Implementation

1. Fernet encryption for sensitive patient data at rest. hashlib is used in which SHA-26 hashing for names with salt protection is implemented for irreversible anonymization (anonymize_name) and Fernet for reversible encryption (encrypt_data/decrypt_data).
2. Data Masking is implemented in contact information masking (emails: ab**@domain.com, phones: XXX-XXX-1234). mask_contact function hides emails and phone numbers (e.g., ab**@domain.com, XXX-XXX-1234)
3. Access Control is ensured using Three-tier RBAC (Admin/Doctor/Receptionist) with strict data segregation. get_permissions() defines what each role can see/do. Admins see raw data, doctors see anonymized data, receptionists can add records but not view sensitive data.
4. Authentication is done using bcrypt password hashing with secure session management.

Integrity Implementation

1. Audit Logging is done by comprehensive tracking of all user actions with timestamps. log_action() function logs all key actions to a logs table with user ID, role, timestamp, and details.
2. Admins can view logs in the "Dashboard" tab. Audit trails cannot be modified or deleted.
3. Data Validation is done using Input validation and database constraints. Uses NOT NULL, CHECK constraints in SQLite.
4. Server-side permission validation for all operations. Validates inputs (e.g., validate_name, validate_contact).

Availability Implementation

1. Robust exception handling blocks throughout the system including DB operations, encryption, and login.
2. Automatic cleanup of expired data (30-day policy).
3. CSV export functionality for data recovery. Admins can export patient data as CSV.

4. Real-time status dashboard with uptime tracking .Sidebar shows system uptime and last sync timestamp.

GDPR Compliance Alignment

Privacy by Design:

- Explicit user consent is taken before data processing.
- Only necessary information is collected.
- Role-based data access controls are implemented throughout the system.
- Automatic data retention and cleanup is ensured.
- Clear privacy notices and data handling explanations are provided.
- Comprehensive audit trails for compliance reporting ensures accountability of the users.

Data Protection Impact:

- All personal data of patients is anonymized, encrypted, or masked
- Regular automatic deletion of expired records is done using data retention
- Role-based access ensures the principle of least privilege, access is restricted based on roles.
- A complete audit trail for regulatory compliance is ensured using activity logs.

Database Schema

Three required tables:

- users (with role and password_hash)
- patients (with both raw and anonymized/encrypted fields)
- logs (with user ID, role, action, timestamp, and details)

Example Workflow

The app mirrors the workflow exactly:

1. Login is done based on the role of the user.
2. Admin has full access to the system including anonymization tools and logs.

3. Doctors are allowed to view anonymized data only.
4. Receptionists can add patients but are not allowed to view personal data.
5. Logging allows all the actions to be recorded.
6. Audit allows the admin to review logs and export data.