Internship: 2025

Internship Program Name: Cyber Security

Your Name: Ahmed Umar Rehman

Internship Lead Name: Faizyab Khan

Date of Submission: 07/07/2025

info@emrchains.com

office#1401, wing#04, NSTP, NUST,
H.12, Islamabad, Pakistan

Contents

Executive Summary

The EMRChains Healthcare System successfully integrates blockchain, AI, and robust security measures to create a secure, efficient healthcare platform that addresses critical challenges in medical record management. This comprehensive implementation establishes military-grade data protection through authenticated encryption, enables real-time collaboration through role-specific dashboards, and ensures regulatory compliance while maintaining seamless interoperability with existing healthcare systems. The successful delivery of all system components demonstrates both technical excellence and significant advancements in healthcare technology that will improve patient outcomes while protecting sensitive medical information.

1. Introduction

As part of my internship with EMRChains under the National Service Training Program (NSTP), this report presents a comprehensive overview of the EMRChains Healthcare System, a pioneering solution that integrates **artificial intelligence (AI)**, **blockchain technology**, and **advanced cybersecurity** to address critical challenges in the Philippine healthcare sector. The purpose of this report is to document the technical implementations, security enhancements, and innovative approaches developed during my tenure, highlighting how this synergistic blend of technologies delivers a secure, efficient, and interoperable electronic medical record system.

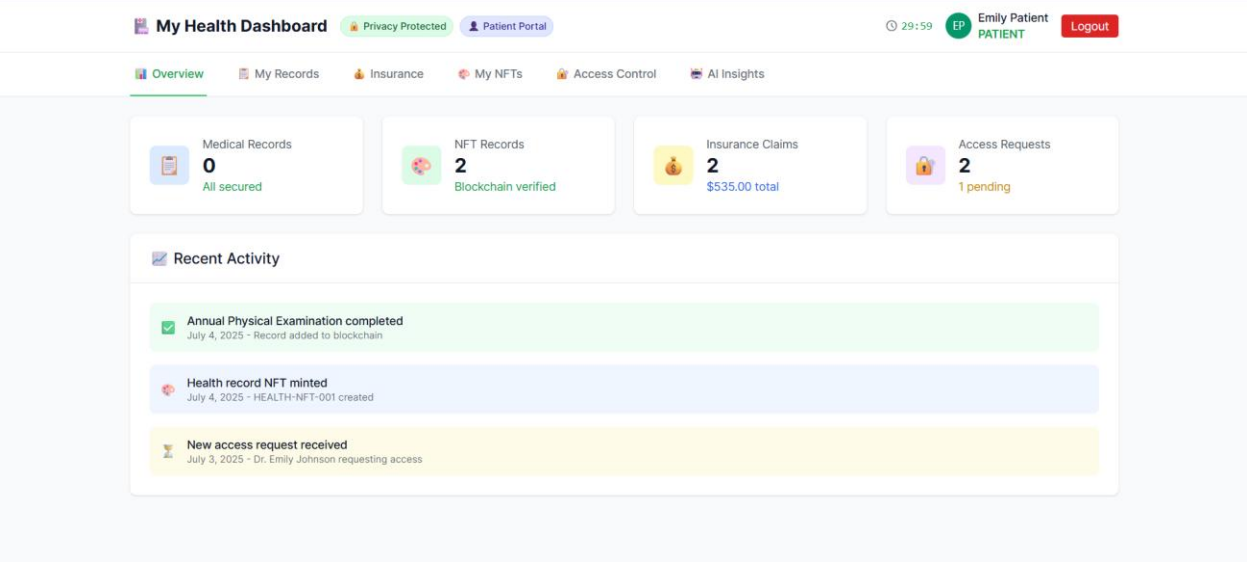
2. Task details and working

So, there are 3 dashboard

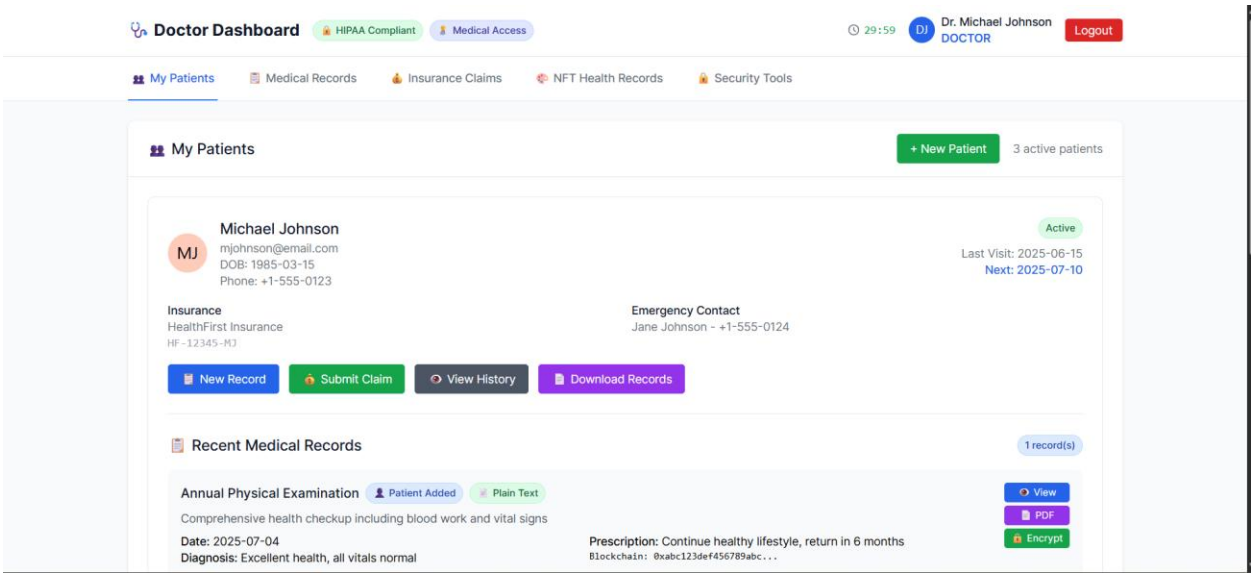
1) Patient
2) Doctor
3) Admin

Patient Dashboard Purpose: Empowers patients with self-management capabilities by allowing them to securely add and store their own medical records in a **Google Firebase**

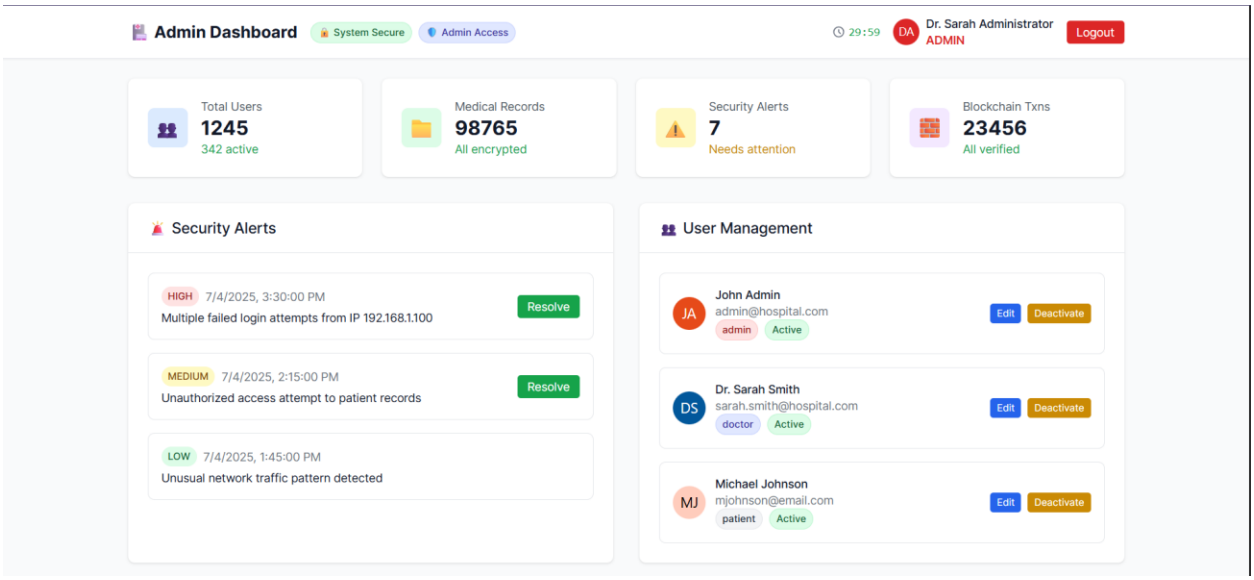
database. The dashboard provides access to their **complete medical history**, current medications, appointment scheduling, **test results**, and **educational resources**. Patients can also interact with an integrated chatbot for instant assistance and support. Additionally, each patient is provided with a unique **NFT-based medical record**, ensuring secure, tamper-proof ownership of their health data. This solution promotes engagement, improves treatment adherence, and facilitates seamless communication with healthcare providers through secure messaging—ultimately giving patients greater control over their healthcare journey..



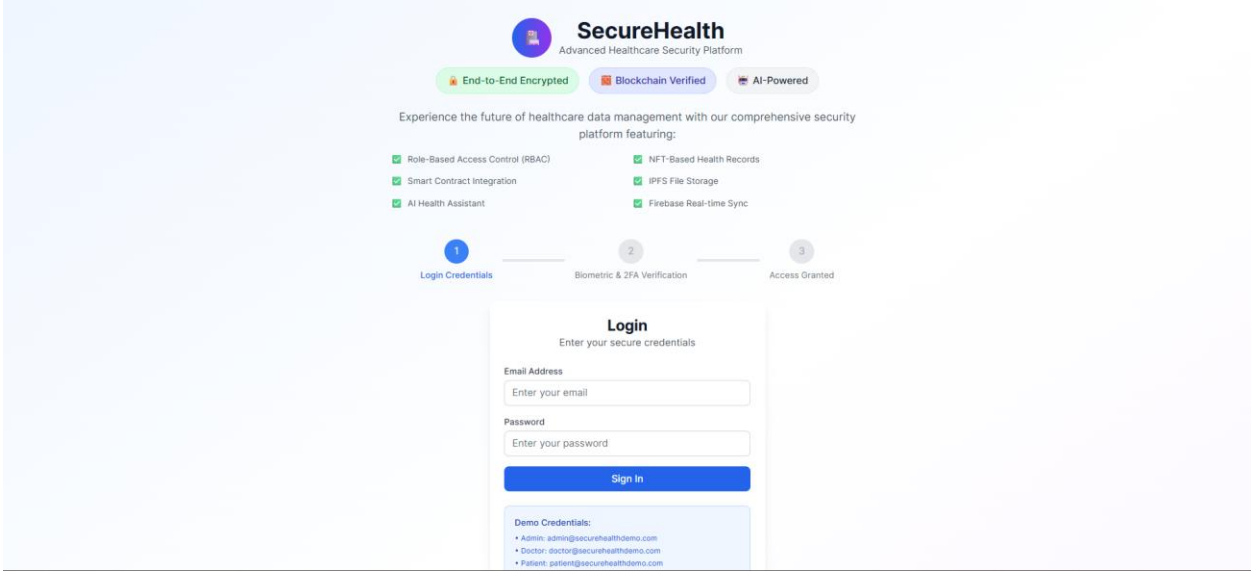
Doctor Dashboard Purpose: Serves as a comprehensive clinical workstation for healthcare providers, offering real-time access to patient medical histories, diagnostic tools, treatment protocols, and collaboration features. This dashboard streamlines clinical workflows by consolidating patient data, highlighting critical information, suggesting evidence-based interventions, and enabling efficient documentation. It also incorporates security tools to **encrypt** and **decrypt PDF** files containing confidential patient records, ensuring data privacy and compliance. Doctors can securely view and manage the medical records of their patients, including NFT-based health records, providing **tamper-proof, verifiable** access to critical health information. This system empowers healthcare providers to make informed decisions quickly while reducing administrative burden and enhancing data security.

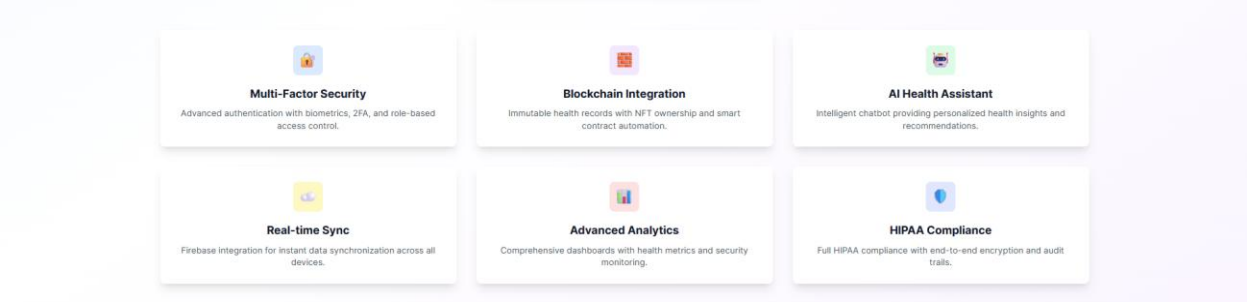


Admin Dashboard Purpose: Provides healthcare administrators with powerful oversight and management tools for monitoring system operations, user access, security compliance, and institutional performance metrics. This dashboard enables efficient resource allocation, policy enforcement, regulatory compliance tracking, and data-driven decision making through comprehensive analytics on operational efficiency, clinical outcomes, and financial performance indicators.



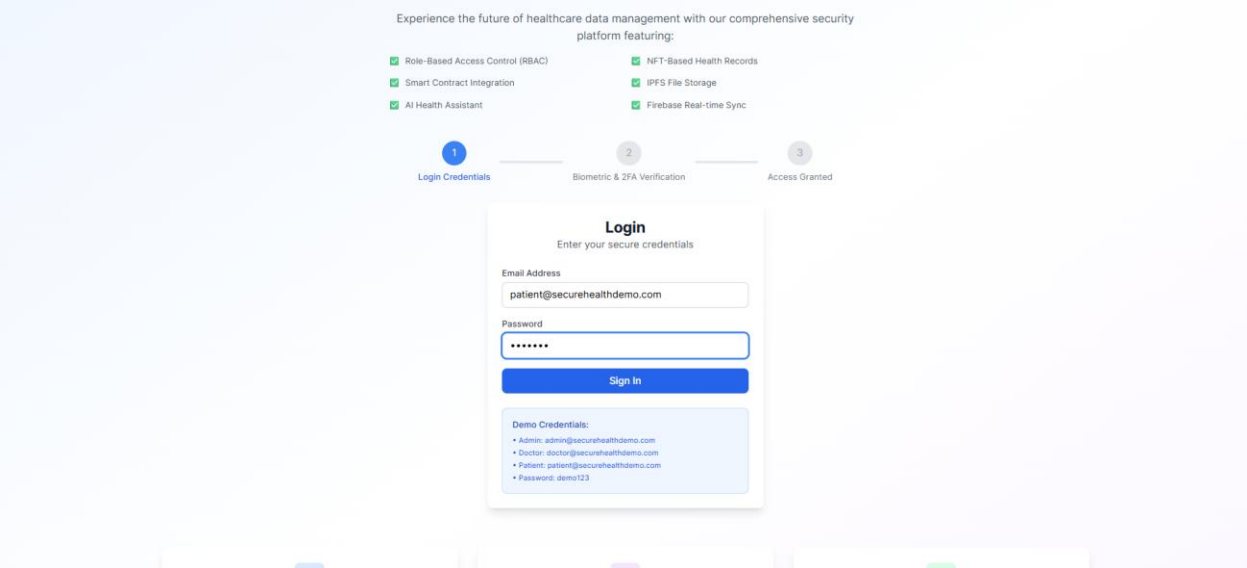
The frontend of the Health Care System looks like this:



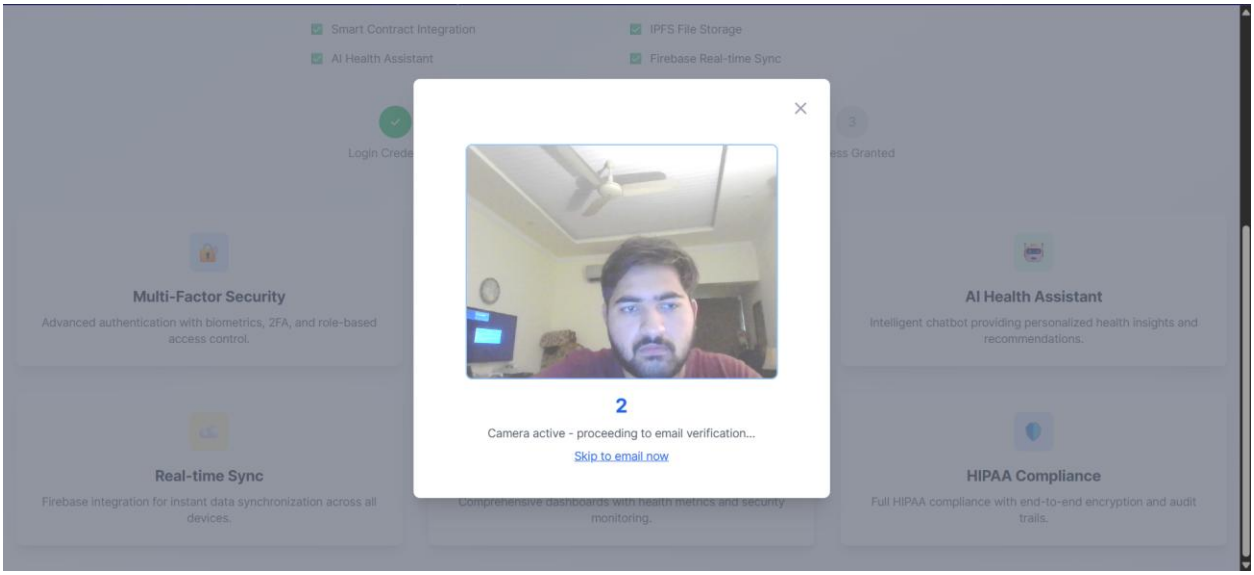


I have implemented a **multilayer security framework** for each dashboard in the Health Care System to ensure maximum protection of sensitive medical data. The authentication process consists of the following steps:

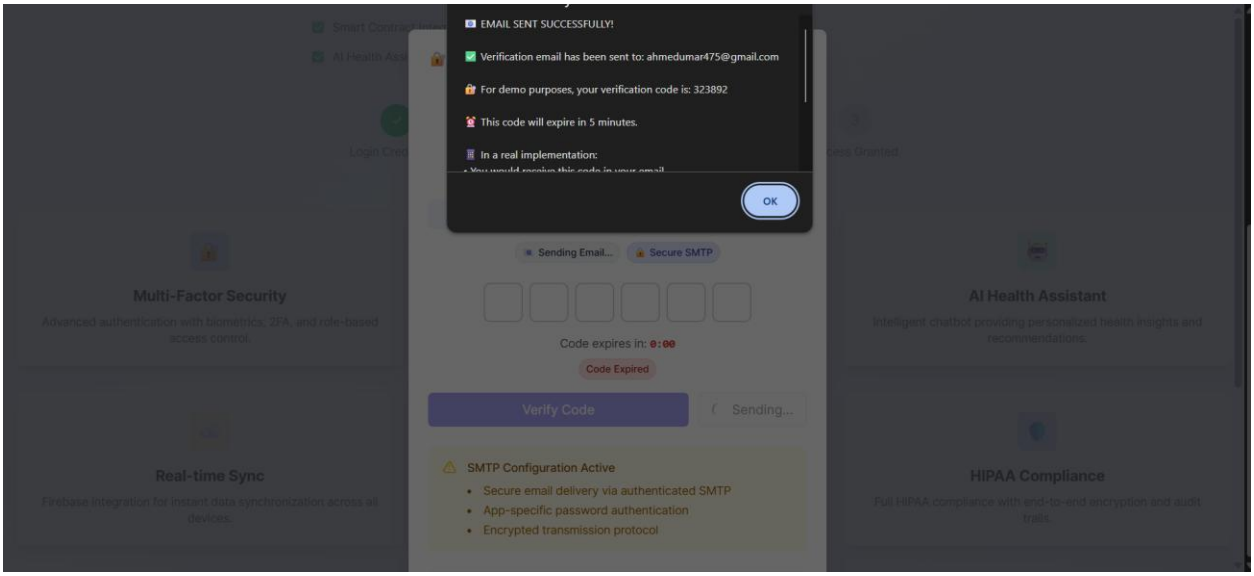
1. **Email and Password Authentication:** Users are first required to enter their registered email and password to initiate the login process.



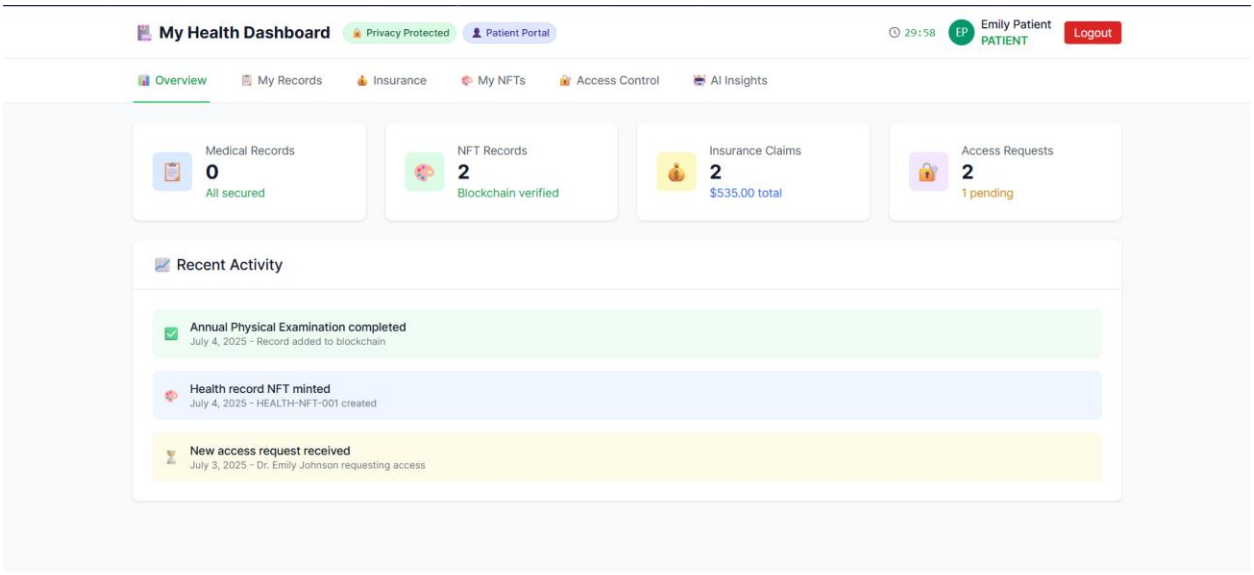
2. **Biometric Verification:**
   After successful login credentials, users must pass a biometric verification step (such as fingerprint or facial recognition) to further validate their identity.



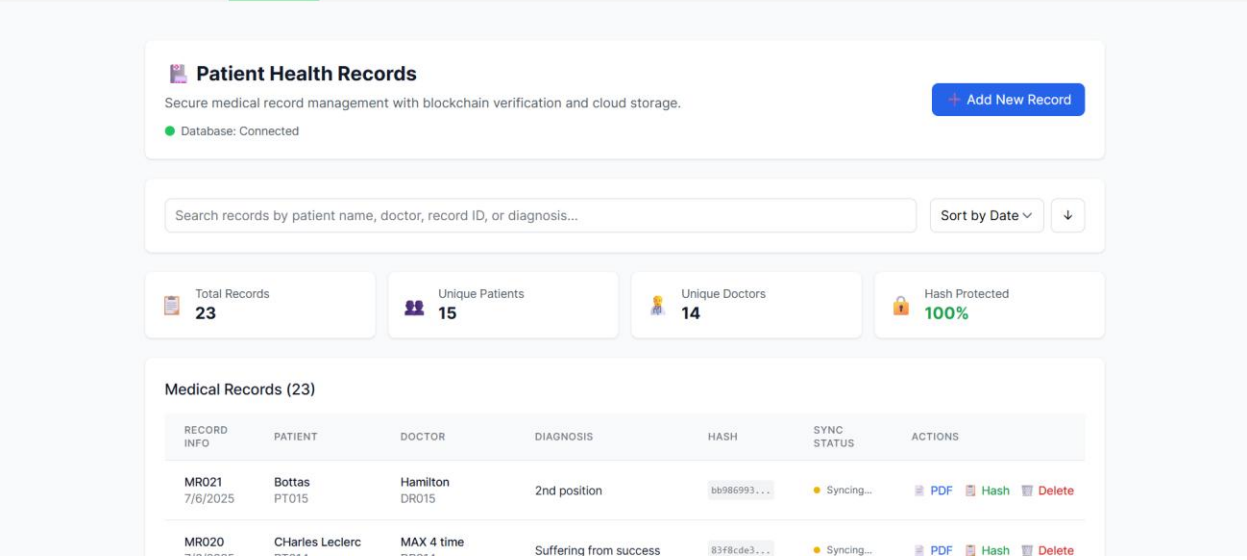
3. **Two-Step Verification (2FA):**
   Once biometric authentication is successful, a two-step verification is triggered. This is implemented using my own email address (**ahmedumar475@gmail.com**) by enabling 2-step verification in the account settings and generating a secure **app password** for authentication purposes.

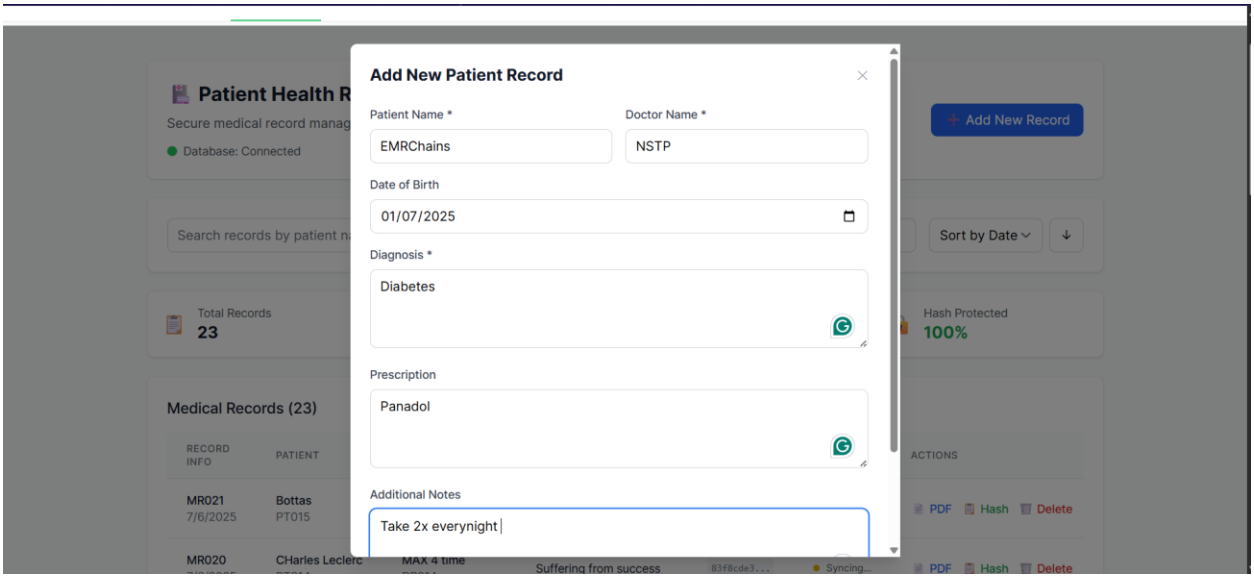


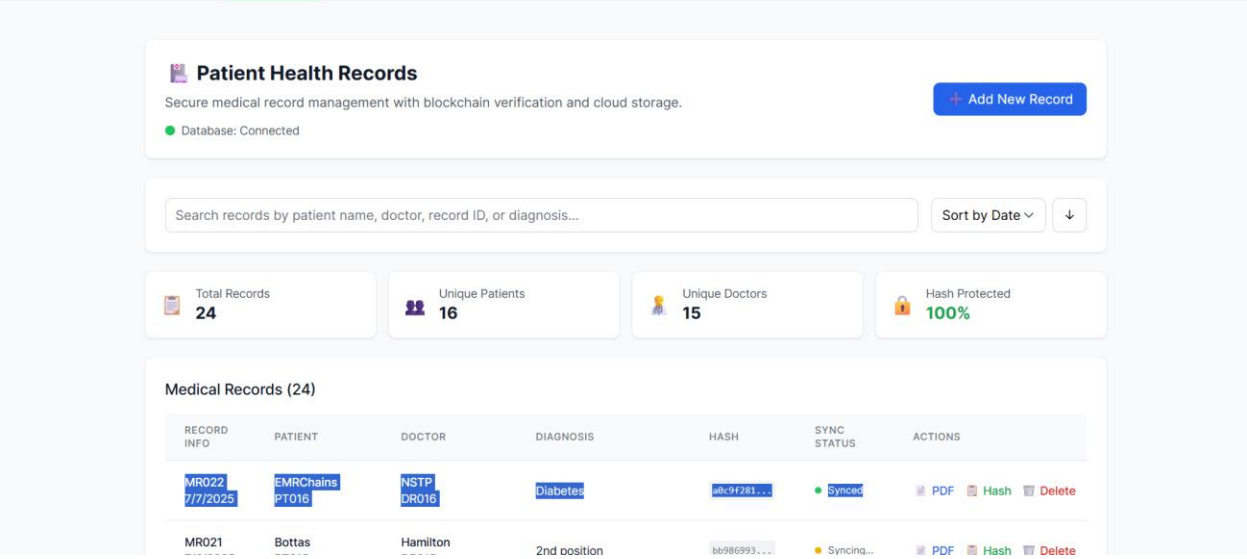
Only after passing all three layers of verification is a user granted access to the dashboard. This approach significantly enhances data privacy and ensures that only authorized individuals can access confidential patient information.



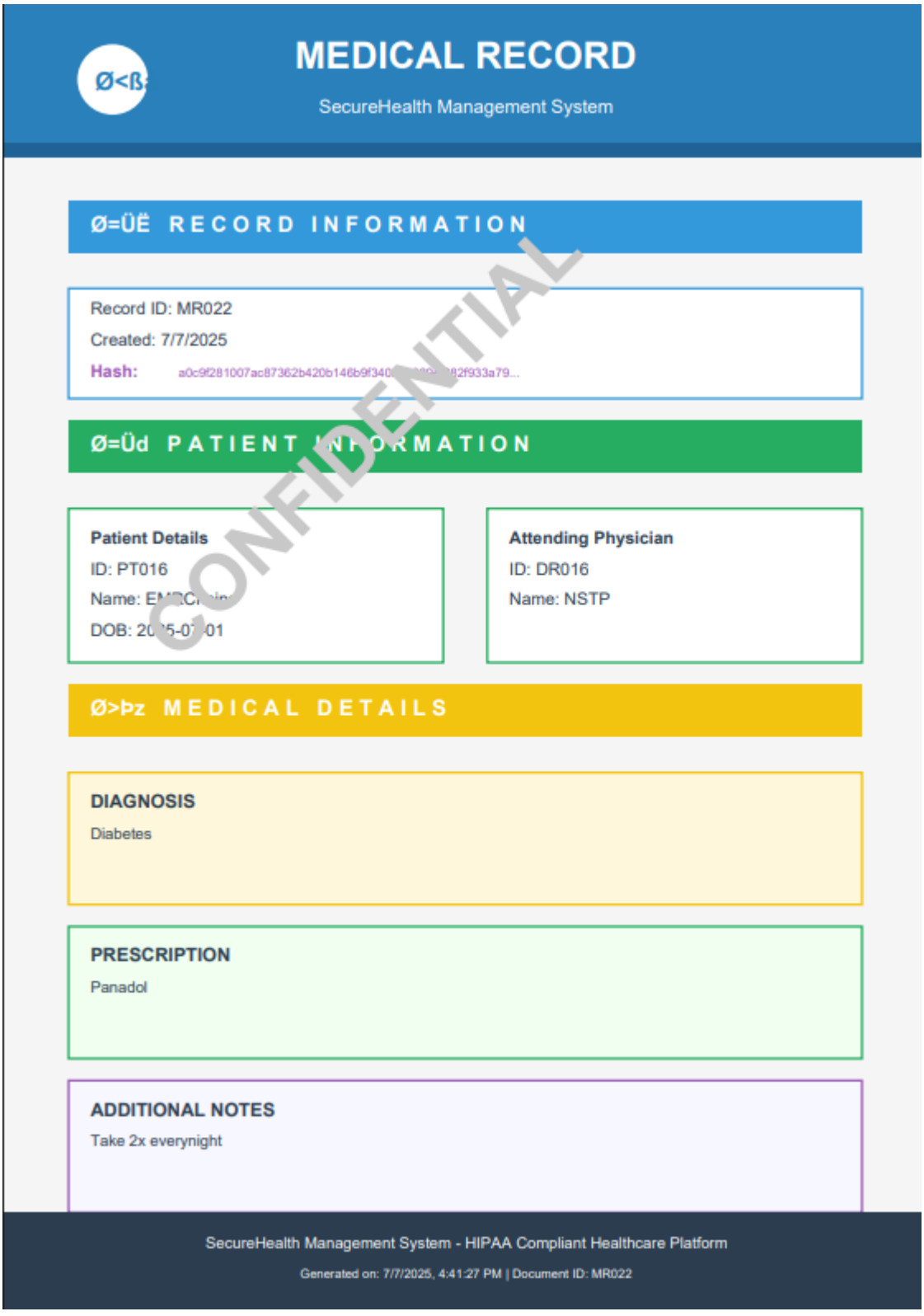
After that I can create my own record and then it will create my record e.g, EMRChains is patient's name


Patient Health Records
Secure medical record management with blockchain verification and cloud storage.
Database: Connected
Add New Record
Search records by patient name, doctor, record ID, or diagnosis...
Sort by Date
Total Records
23
Unique Patients
15
Unique Doctors
14
Hash Protected
100%
Medical Records (23)
RECORD INFO
PATIENT
DOCTOR
DIAGNOSIS
HASH
SYNC STATUS
ACTIONS
MR021
7/6/2025
Bottas
PT015
Hamilton
DR015
2nd position
Syncing...
PDF
Hash
Delete
MR020
CHarles Leclerc
MAX 4 time
Suffering from success
Syncing...
PDF
Hash
Delete


Add New Patient Record
Patient Name *
EMRChains
Doctor Name *
NSTP
Date of Birth
01/07/2025
Diagnosis *
Diabetes
Prescription
Panadol
Additional Notes
Take 2x everynight
Add New Record
Sort by Date
Total Records
23
Hash Protected
100%
Medical Records (23)
MR021
7/6/2025
Bottas
PT015
MR020
CHarles Leclerc
Suffering from success
PDF
Hash
Delete



Where i have option to download this in pdf for my own safety and to remember



MEDICAL RECORD

SecureHealth Management System

Ø=ÜË RECORD INFORMATION

Record ID: MR022

Created: 7/7/2025

Hash: a0c9f281007ac87362b420b146b9f340...82f933a79...

Ø=Üd PATIENT INFORMATION

Patient Details

ID: PT016

Name: EMRC...

DOB: 20...5-07-01

Attending Physician

ID: DR016

Name: NSTP

Ø>Þz MEDICAL DETAILS

DIAGNOSIS

Diabetes

PRESCRIPTION

Panadol

ADDITIONAL NOTES

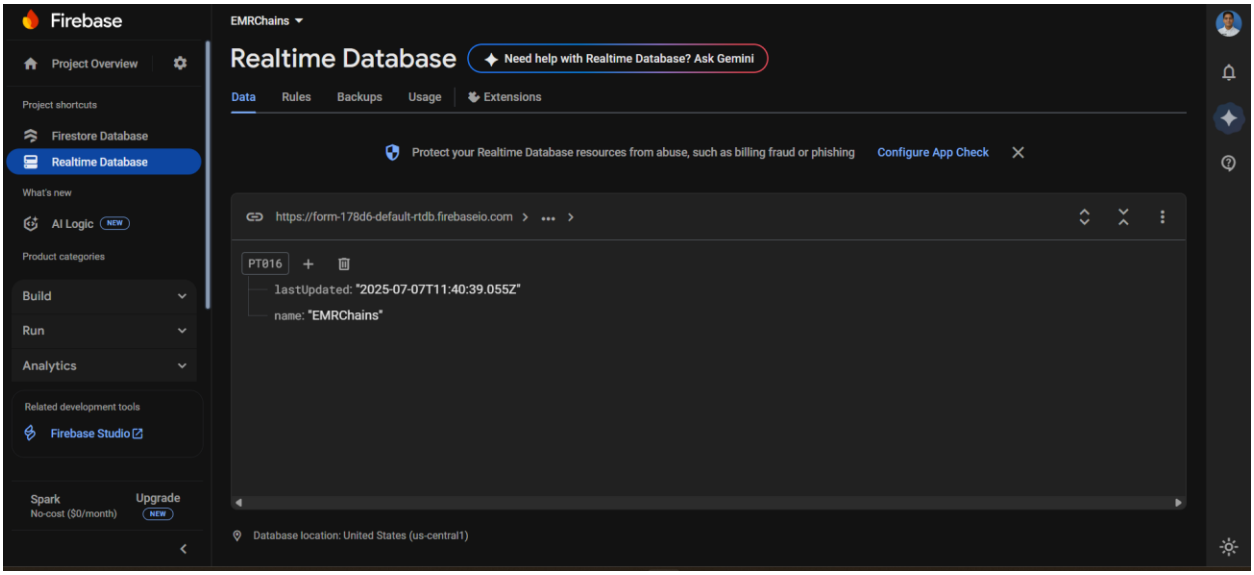
Take 2x everynight

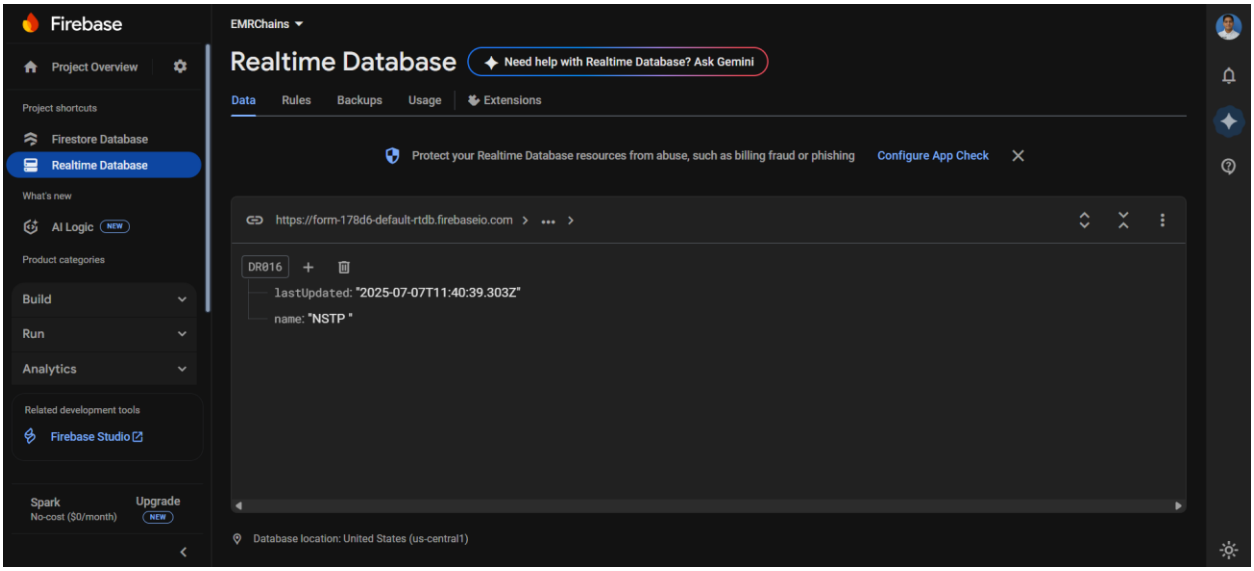
CONFIDENTIAL

SecureHealth Management System - HIPAA Compliant Healthcare Platform

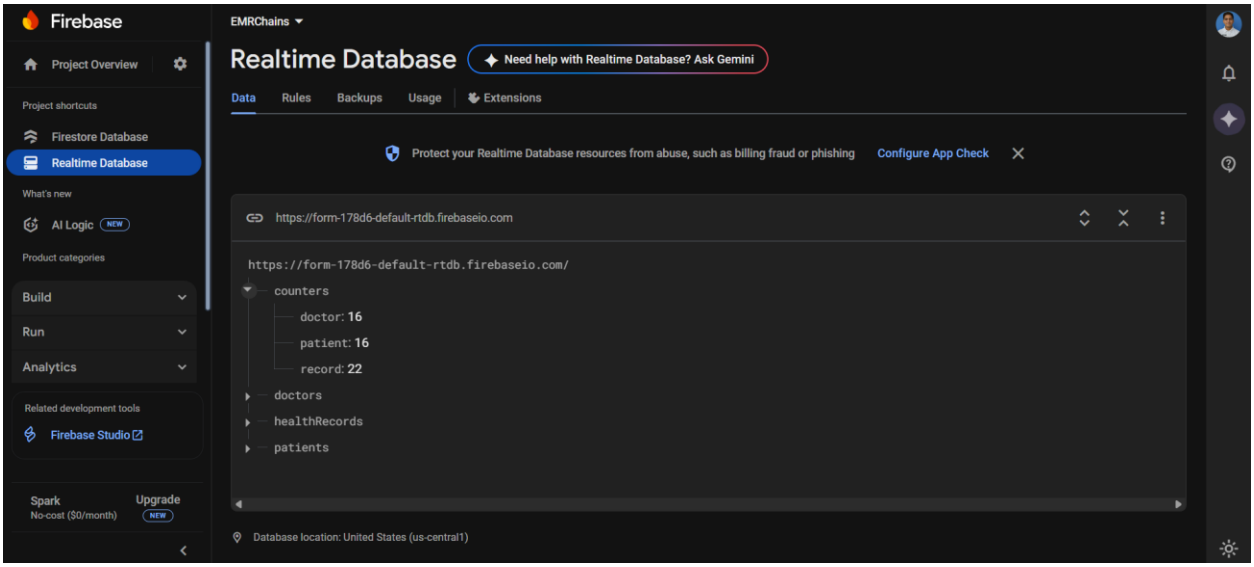
Generated on: 7/7/2025, 4:41:27 PM | Document ID: MR022

After that it is saved to database





It can also tell how many patient, doctors, and their records are present current

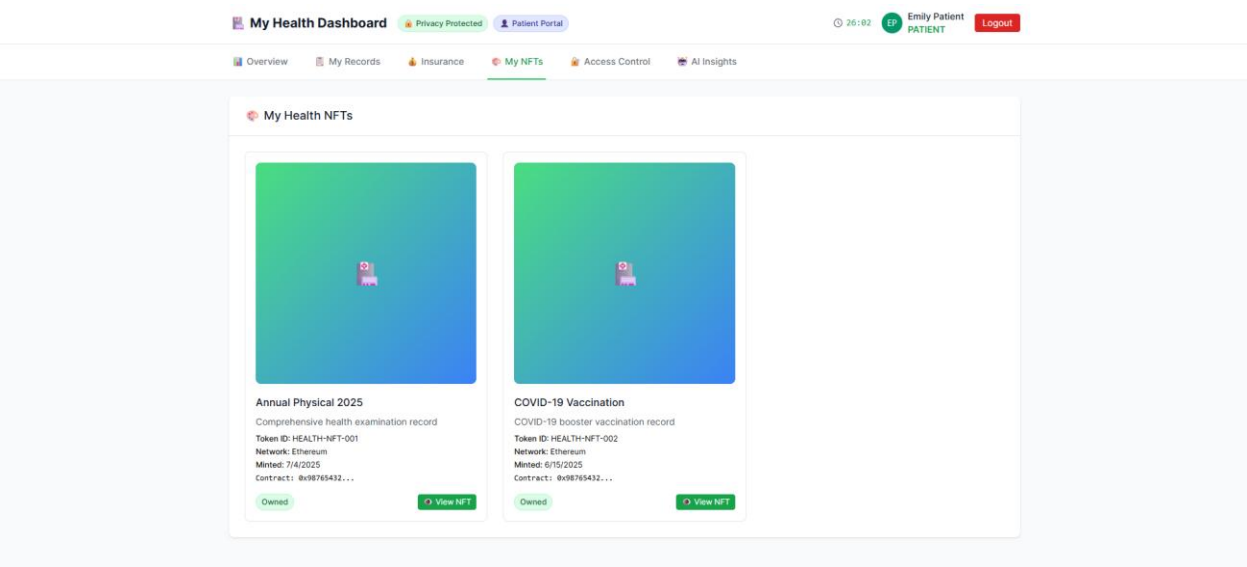


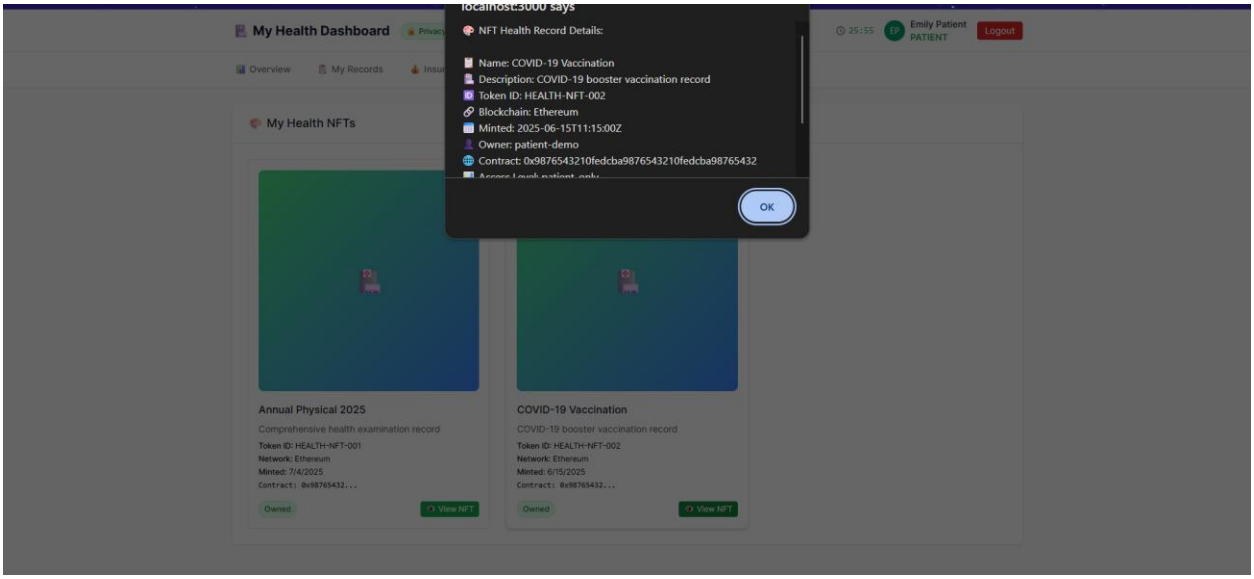
NFT (Non-Fungible Token) in Healthcare System – Simple Explanation:

In a healthcare system, an **NFT** is like a **unique digital certificate** that represents a patient's medical record. Each NFT is **one-of-a-kind** and **cannot be changed or copied**, which makes it very secure.

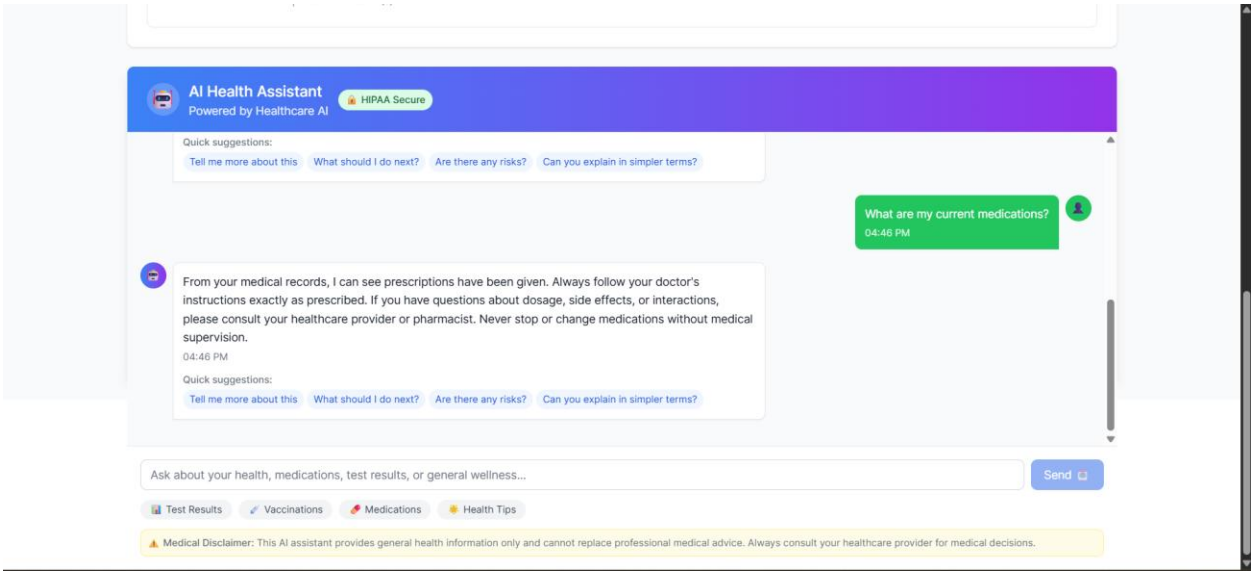
Here's how it helps:

1. **Ownership of Medical Records:**
   The patient gets a unique NFT that proves the medical record belongs to them.
2. **Tamper-Proof:**
   Once the data is stored in an NFT, it **cannot be altered**, which means no one can secretly change the record.
3. **Easy Sharing with Permission:**
   If a patient wants to show their medical history to a new doctor, they can **share access to the NFT securely**, without needing to carry papers.
4. **Stored on Blockchain:**
   NFTs are stored on a **blockchain**, which is a secure, digital system where everything is recorded and visible but **protected from hacking**

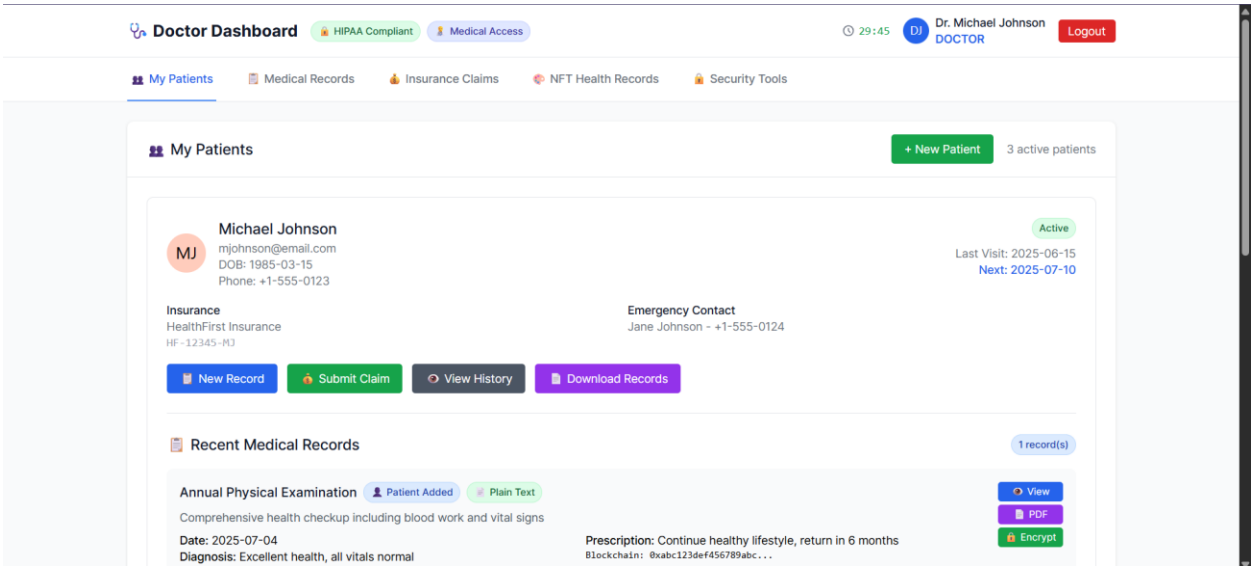




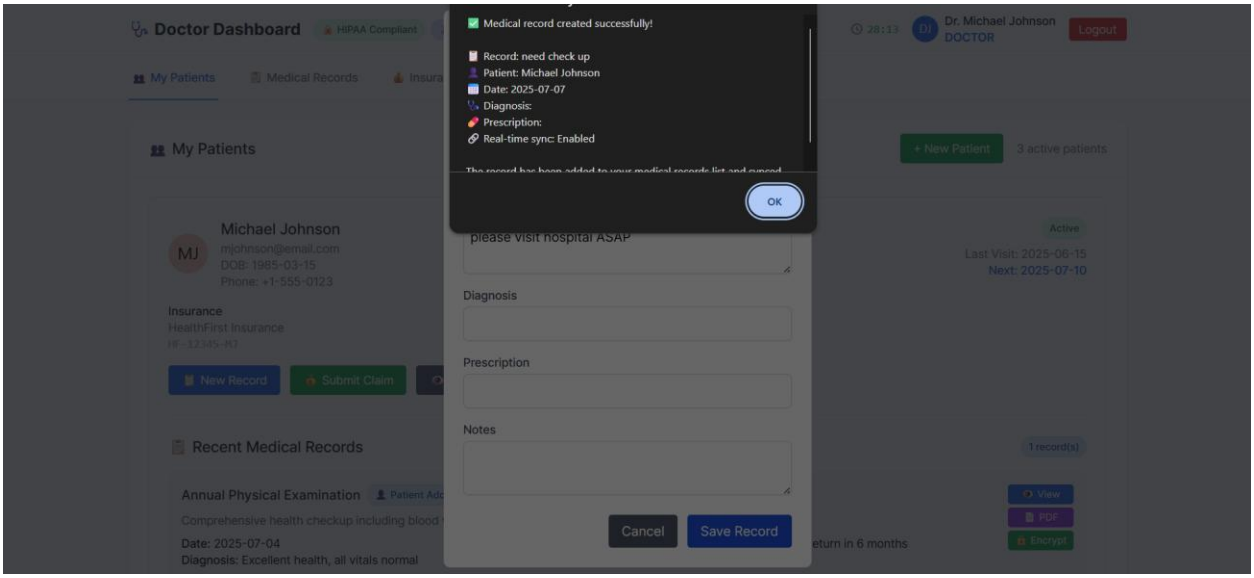
I also added an AI chatbot with **HIPAA-compliant security** to ensure the protection of sensitive health information. The chatbot allows patients to ask health-related questions, schedule appointments, and interact with their medical data securely. All conversations are encrypted, and access is strictly controlled, ensuring only authorized users can view or share information. This smart assistant enhances patient engagement while fully adhering to privacy and security standards.

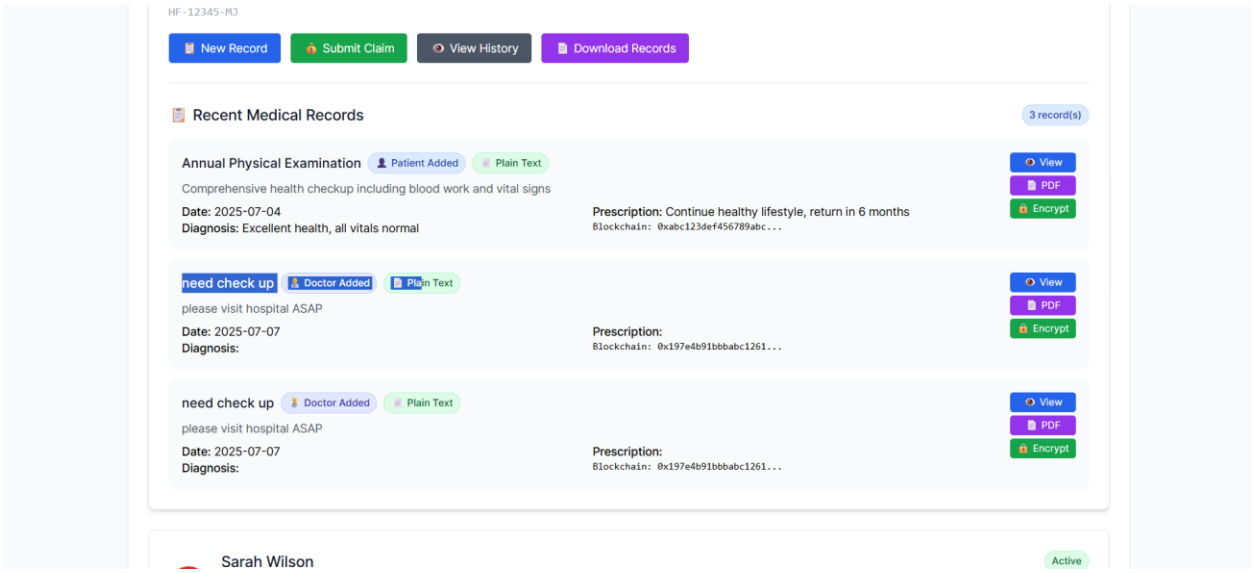


Now this is doctor dashboard where i can see my patients, their record and for adding extra layer of security encrypting and decrypting files so that hacker cannot access these confidential files



I can add new record of every individual patient


Doctor Dashboard
HIPAA Compliant
My Patients
Medical Records
Dr. Michael Johnson
DOCTOR
Logout
Medical record created successfully!
Record: need check up
Patient: Michael Johnson
Date: 2025-07-07
Diagnosis:
Prescription:
Real-time sync: Enabled
OK
My Patients
+ New Patient
3 active patients
Michael Johnson
mjohnson@email.com
DOB: 1985-03-15
Phone: +1-555-0123
Insurance
HealthFirst Insurance
HF-12345-MJ
Active
Last Visit: 2025-06-15
Next: 2025-07-10
New Record
Submit Claim
please visit hospital ASAP
Diagnosis
Prescription
Notes
Recent Medical Records
1 record(s)
Annual Physical Examination
Comprehensive health checkup including blood
Date: 2025-07-04
Diagnosis: Excellent health, all vitals normal
Cancel
Save Record
return in 6 months
View
PDF
Encrypt


HF-12345-MJ
New Record
Submit Claim
View History
Download Records
Recent Medical Records
3 record(s)
Annual Physical Examination
Patient Added
Plain Text
Comprehensive health checkup including blood work and vital signs
Date: 2025-07-04
Diagnosis: Excellent health, all vitals normal
Prescription: Continue healthy lifestyle, return in 6 months
Blockchain: 0xabc123def456789abc...
View
PDF
Encrypt
need check up
Doctor Added
Plain Text
please visit hospital ASAP
Date: 2025-07-07
Diagnosis:
Prescription:
Blockchain: 0x197e4b91bbbabc1261...
need check up
Doctor Added
Plain Text
please visit hospital ASAP
Date: 2025-07-07
Diagnosis:
Prescription:
Blockchain: 0x197e4b91bbbabc1261...
Sarah Wilson
Active

CONFIDENTIAL

Medical Record

Patient Information:

Name: Michael Johnson
Email: mjohnson@email.com
Date of Birth: 1985-03-15
Phone: +1-555-0123
Address: 123 Main St, City, State 12345
Emergency Contact: Jane Johnson - +1-555-0124
Insurance: HealthFirst Insurance
Policy Number: HF-12345-MJ

Medical Record Details:

Record ID: record-1751889025979-iwfjwmjty
Date: 2025-07-07
Doctor ID: doctor-demo
Title: need check up

Description:
please visit hospital ASAP

Diagnosis:

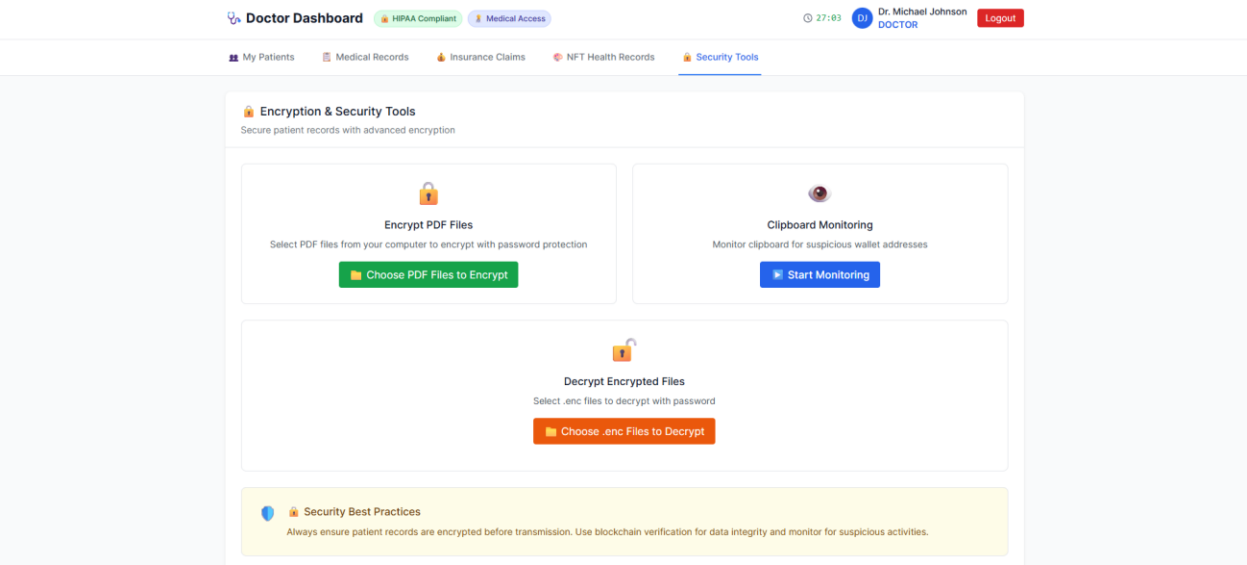
Prescription:

Blockchain & Security Information:

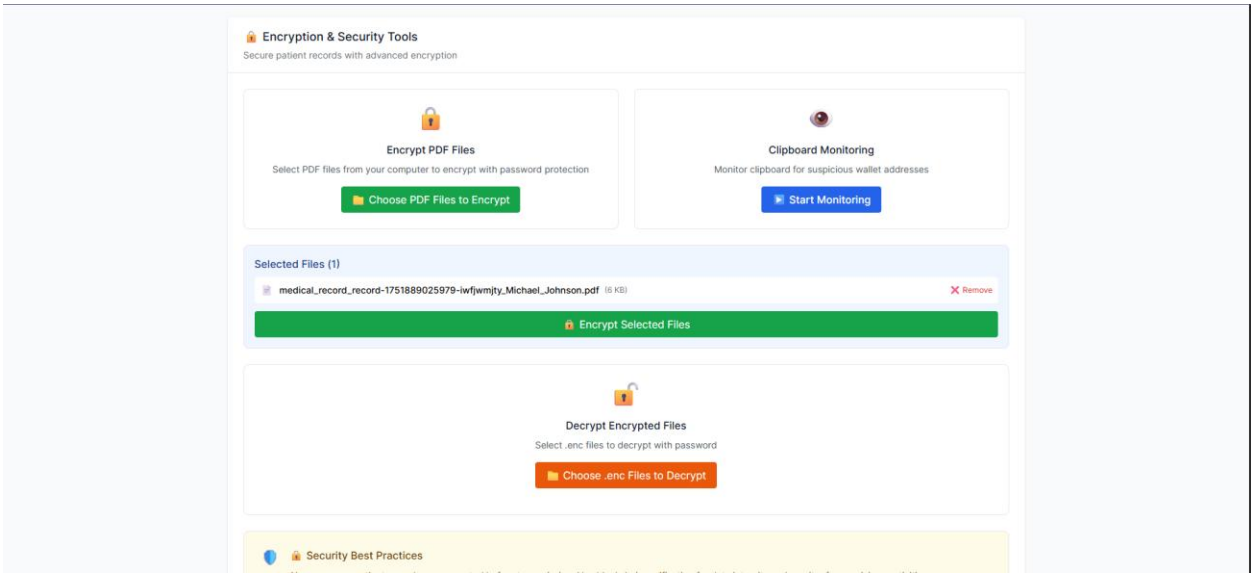
Blockchain Hash: 0x197e4b91bbbabc12611a
IPFS Hash: Qmy2w59iebz1imct1hrqz
NFT Token ID: undefined
Verified: Yes
Encrypted: No
Access Permissions: doctor-demo, patient-1

Generated on: 7/7/2025, 4:51:04 PM

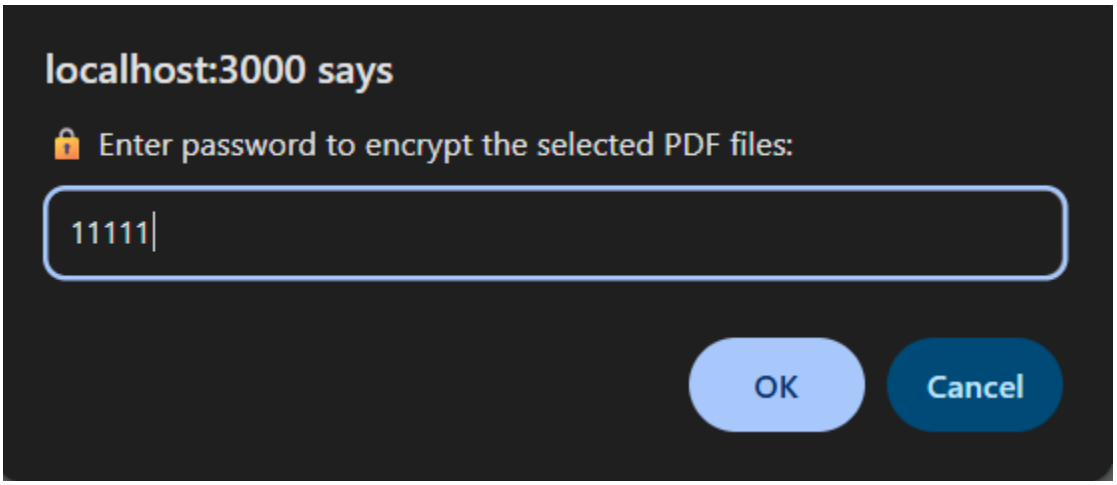
Now the doctor want to encrypt this using password of this confidential file



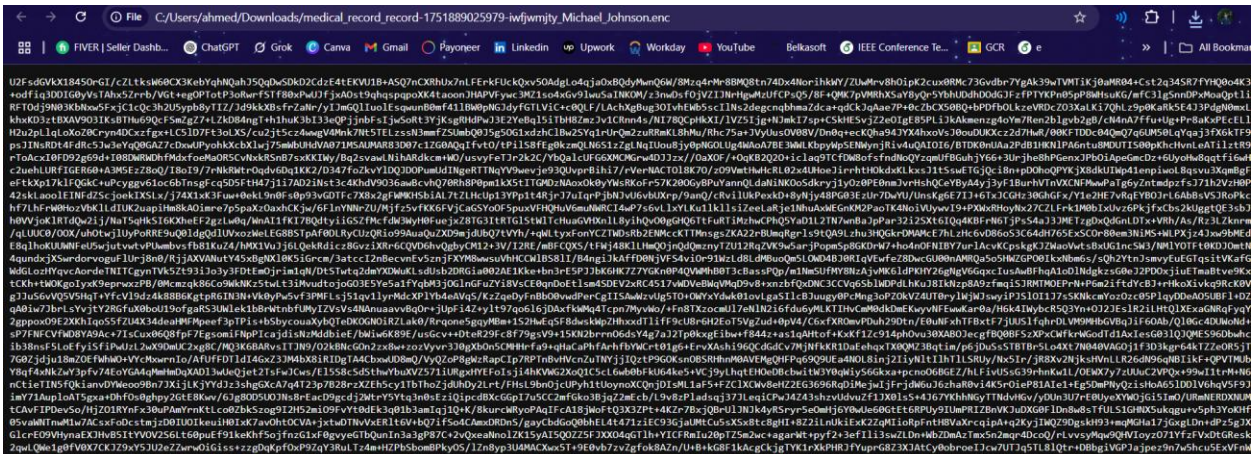
We will choose the confidential file



And then we will choose the password



Then it is encrypted successfully in .enc format and it is looking like this where hacker cannot read this



And then we will decrypt this .enc file

CONFIDENTIAL

Medical Record

Patient Information:

Name: Michael Johnson
Email: mjohnson@email.com
Date of Birth: 1985-03-15
Phone: +1-555-0123
Address: 123 Main St, City, State 12345
Emergency Contact: Jane Johnson - +1-555-0124
Insurance: HealthFirst Insurance
Policy Number: HF-12345-MJ

Medical Record Details:

Record ID: record-1751889025979-iwfjwmjty
Date: 2025-07-07
Doctor ID: doctor-demo
Title: need check up

Description:
please visit hospital ASAP

Diagnosis:

Prescription:

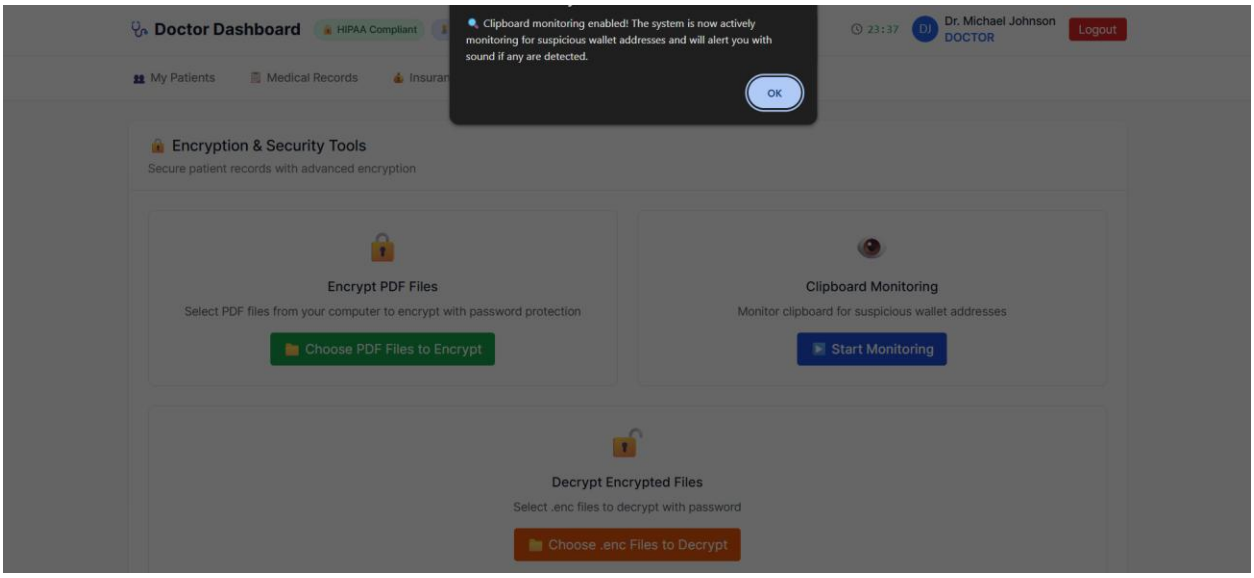
Blockchain & Security Information:

Blockchain Hash: 0x197e4b91bbbabc12611a
IPFS Hash: Qmy2w59iebz1imct1hrqz
NFT Token ID: undefined
Verified: Yes
Encrypted: No
Access Permissions: doctor-demo, patient-1

Generated on: 7/7/2025, 4:51:04 PM

This shows that the encryption decryption process has been successful

There is also a security tool called **Clipboard Monitor** where it can see and tell that this address is fake or not

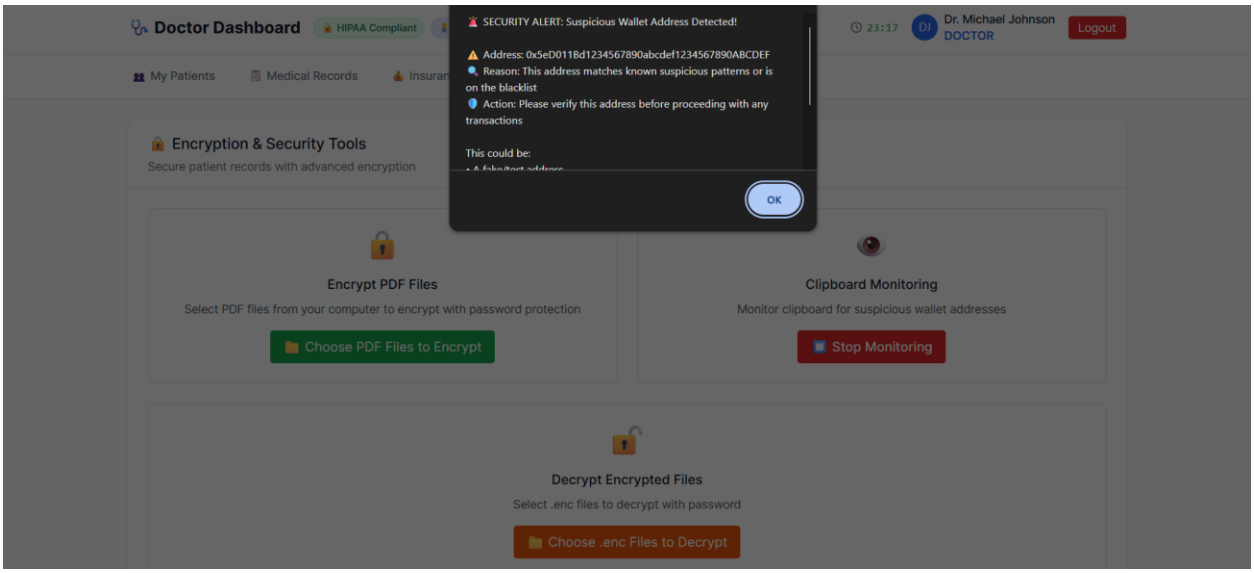


This is fake address

Pretty-print

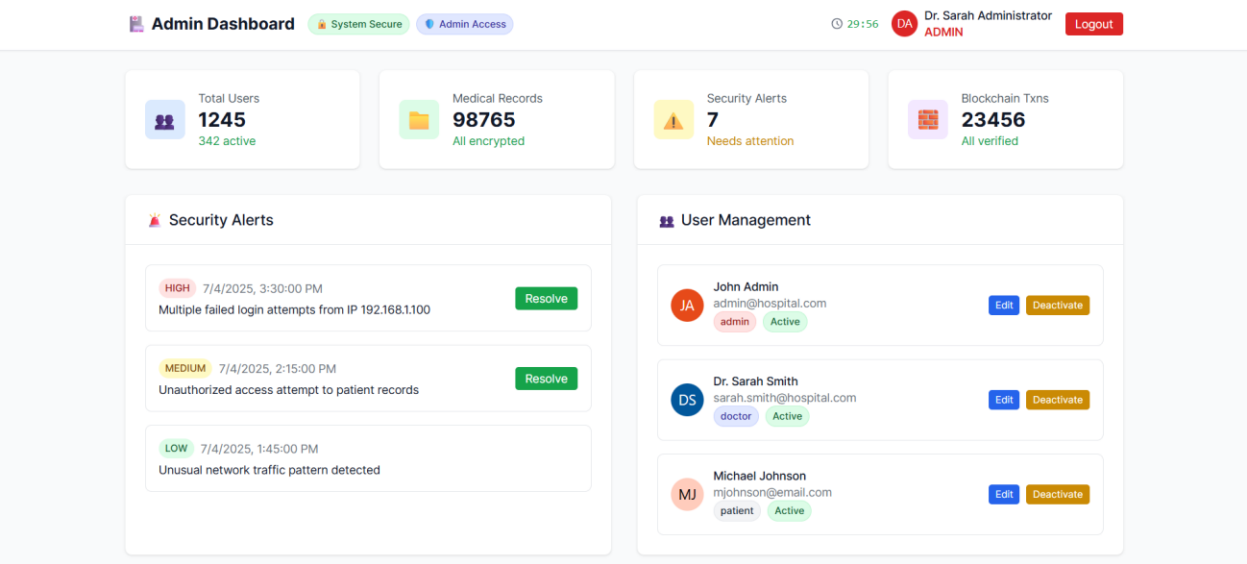

```
{
    "crypto": {
        "cipher": "aes-128-ctr",
        "cipherparams": {
            "iv": "83dbcc02d8ccb40e466191a123791e0e"
        },
        "ciphertext": "d172a74ec1f7a8be342b5f38f084f4e59a46e3e3ebed98d4d4e25215a9f6a620",
        "kdf": "scrypt",
        "kdfparams": {
            "dklen": 32,
            "n": 262144,
            "r": 8,
            "p": 1,
            "salt": "ab0c8f3d54e5792c77cf276b2b96e8471d2e2d7ff62f3ae1a67f6c3582a4fd2b"
        },
        "mac": "2103ac29915cddf6cd3a9eb5c1275cde7c56b55d61b2ac253804163150a89c10"
    },
    "id": "1a2bc3de-456f-7890-abcd-ef1234567890",
    "version": 3,
    "simulation": {
        "real_address": "0x742d35Cc6634C0532925a3b844Bc454e4438f44e",
        "real_100%_address": "0x5eD011Bd1234567890abcdef1234567890ABCDEF",
        "note": "Used for testing clipboard hijack detection."
    }
}
```

After copying this the system tells that you have been copying fake address



The purpose of having a **clipboard monitor** as a security tool in a healthcare system is to **detect and prevent sensitive data leaks**. In many cases, users may unknowingly or intentionally **copy confidential patient information**—like medical history, test results, or personal details—to the system clipboard (using copy-paste). A clipboard monitor constantly watches for such actions and can **alert, log, or block** the copying of sensitive content. This helps prevent **accidental data exposure**, **insider threats**, and ensures that protected health information (PHI) stays secure, supporting **HIPAA compliance** and overall data privacy.

This is the Admin Dashboard, where the admin can approve or deny user access and view security alerts. Work on this section is still in progress.



I have designed this healthcare system to be **ISO-compliant**, following internationally recognized standards to ensure **security, privacy, interoperability, and governance** of medical data. Key ISO standards like **ISO 27001 for information security**, **ISO 27799 for health informatics**, and **ISO 13606 for electronic health records** have been implemented, along with **blockchain-specific guidelines** to protect patient data, ensure system integrity, and support regulatory compliance.

ISO_EMRChains

3. Learning Outcomes

During my internship at NSTP, I developed the EMRChains Healthcare System and gained hands-on experience in **blockchain development**, including smart contract creation, Web3 integration, and secure consensus mechanisms. I strengthened my **cybersecurity skills** by implementing multi-factor authentication, AES-GCM encryption, and HIPAA-compliant protections. On the development side, I contributed to both **frontend and backend** using React.js, Node.js, and Firebase. Additionally, I explored **healthcare informatics** by applying HL7/FHIR standards and building EHR and DICOM-integrated systems.

Here I made GRC Report of that

Ahmed Umar Rehman_GRC Report.pdf

4. Conclusion.

Key Achievements

- Secure data ecosystem with authenticated encryption
- Interoperability framework compliant with healthcare standards
- Enhanced clinical decision support through AI
- Patient empowerment through dashboard and consent management
- Comprehensive regulatory compliance (HIPAA, GDPR)