CSE 545: Software Security

Secure Hospital System

User Guide – Group 9

Yash Bhokare (L)	Kiran Shanthappa (DL)	Anthony Mac
Sai Manoja Gadde	Shashank Baradi	Karan Naik
Jayanth Goritha	Bhaskara Atluri	Rajesh Badugula

1. Technologies Used

With advances in healthcare informatics, one can provide better means to process patient records and therefore speed up the treatment, which in turn reduces the overall cost. Many tools exist for facilitating patient record processing: from assisting data entry to manipulating records, from generating output in required form to transferring it to other physicians for further examination, or to save it digitally for future use.

1.1 UI Design

Wireframes are used to design the secure hospital system functionality. A wireframe is a two-dimensional depiction of a page's interface that focuses on content priority and space allocation, as well as available features and planned behaviours. Because of this, wireframes rarely incorporate any styling, colour, or images.

Angular has a well-designed framework that makes it simple to use. It was created to enable working with web apps easier using the MVC architecture. It separates the model from the view and manages any data binding issues. Angular also includes two-way data binding, which means that when data in the model changes, the view is instantly updated, and vice versa. Angular was built with efficiency in mind. It is quick and efficient, making it an excellent choice for high-traffic websites. As a result, it is an excellent choice for public-facing websites.

1.2 Application Design

The framework used for backend development of the application is ‘spring boot’ (Java). Spring boot provides reliable performance with security for the application. JWT authentication is currently used for sign-up/sign-in for different user roles. The application uses the JDBC template for interaction with the database. Amazon SQS is used for interaction with the blockchain.

We employ a semi-supervised ML approach to group together malicious IPs. For each IP, we use the labels we must find features that are helpful in separating the good IPs from the bad ones. Another example of machine learning in this project is chatbot. Amazon Lex follows the basic chatbot architecture adhered to by all the big cloud based Conversational AI providers.

1.3 Database Design

The various transaction and user data are captured through the data in the Database. The relation between tables can be seen in the ER diagram below. Here, PostgreSQL will be

hosted in an AWS EC2 instance, with the access from the application for data processing. Hyperledger Fabric used as a solution to overcome the problems of traditional records management in hospital/medical system such as accessibility, security, and transaction/approval records.

2. What's new feature

SHS can be divided into a 3-tier architecture, involving web, app, and data tier. All tiers will be hosted on AWS. The app tier components developed in spring boot and services are up 24/7. The data tier has two components for storing the hospital data. Postgre SQL for storing the hospital data and Hyperledger blockchain to capture the approved transaction details.

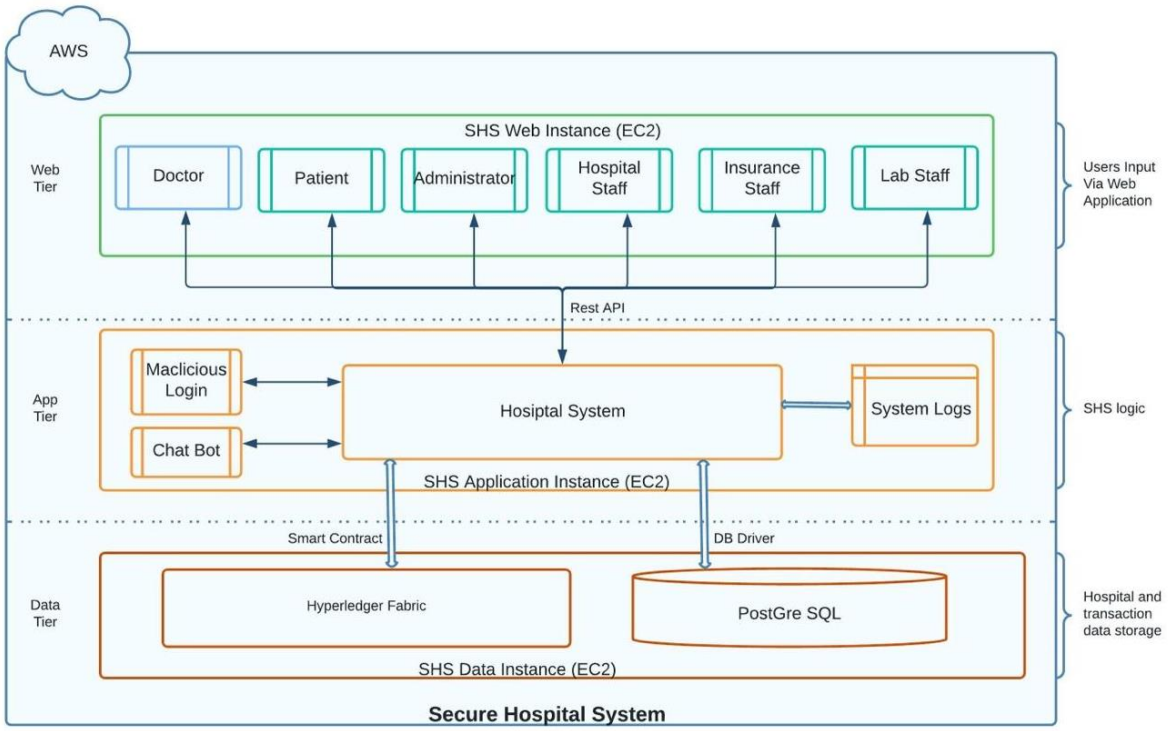


Fig. Secure Hospital System Architecture

The Web application are hosted as website. Web pages are designed using angular, as it is highly preferable as a robust frontend tool supplying components that assist people to write easy-to-use, readable, and maintainable code. Angular has built-in support to help prevent two common HTTP vulnerabilities, cross-site request forgery (CSRF or XSRF) and cross-site

script inclusion (XSSI). Both must be mitigated primarily on the server-side, but Angular provides helpers to make integration on the client-side easier.

Wireframe designs for the secure hospital functionality are provided below as a reference:

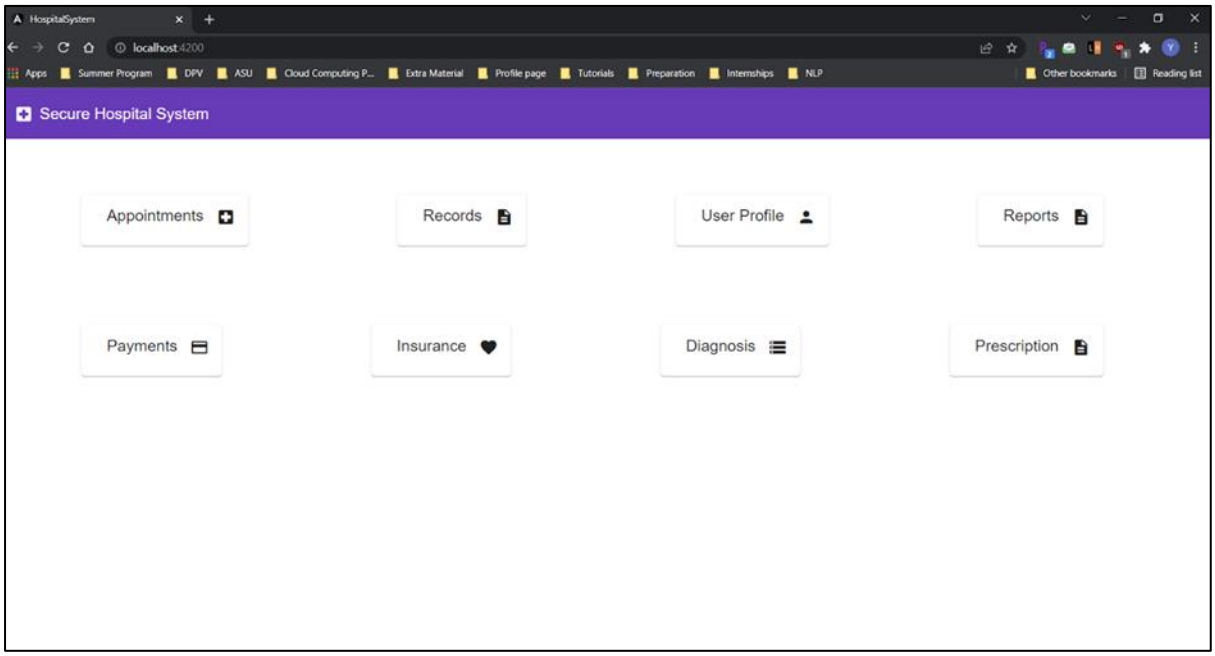


Fig. Wireframe Design - Dashboard

A security group acts as a virtual firewall for SHS EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. When component launched as an instance, you can specify same security groups. All components access across tier will be through secure protocol such as HTTPS. The secure hospital system will use a certificate for the web application for accessing webpages. A key pair, consisting of a public key and a private key, is a set of security credentials that you use to prove your identity when connecting to an Amazon EC2 instance. Amazon EC2 stores the public key on your instance, and you store the private key.

Blockchain technology is based on the principle of providing an individual control over their data and information, and hence potentially appropriate as part of a solution to patient ownership of their health data. Blockchain can create a decentralized identification that allows health care providers and patients to interact with one another directly without the need for an intermediary. The immutable audit trail which allows all changes of personal information to be tracked and traced. The increased security of patient's medical information. Not only is the data stored in multiple nodes across the distributed ledger; but it can also be encrypted with

the only key being in the hands of the patient. Due to limited functionality the feature of key with patient will be considered as future work. Blockchain applications may, therefore, provide solutions to the current problems of interoperability of medical records, incomplete patient data at the point of service, integrate insurance claim, and lack of access to personal records while ensuring security.

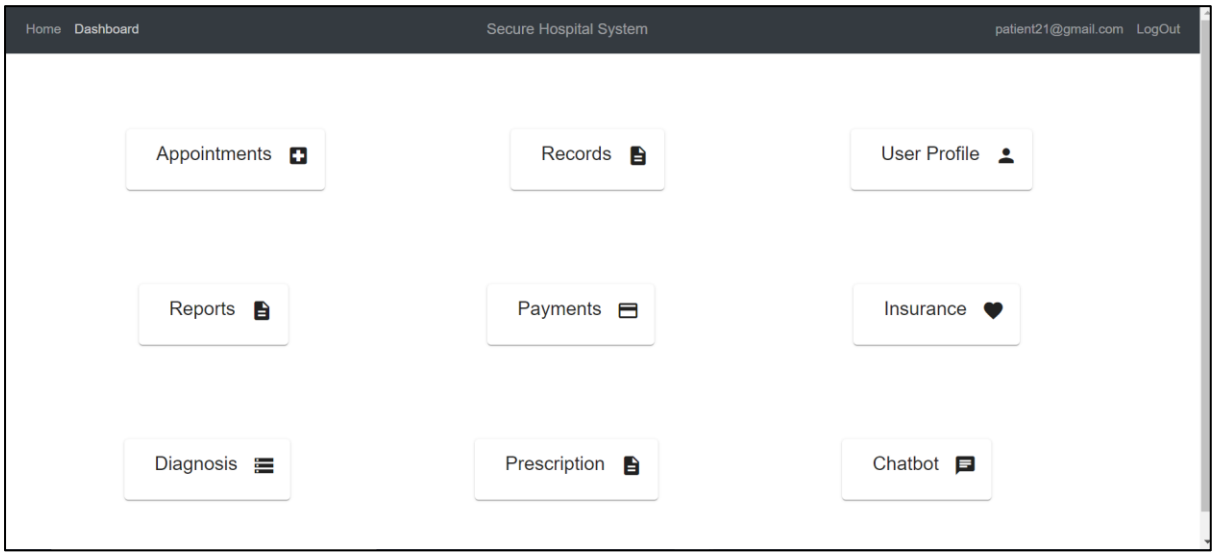
3. Workflow by User Operation

For accessing secure hospital system, user has to sign-up with relevant role. Login to the SHS using login authentication and two-factor authentication. Following subsection describes the functionality and navigation for various user roles.

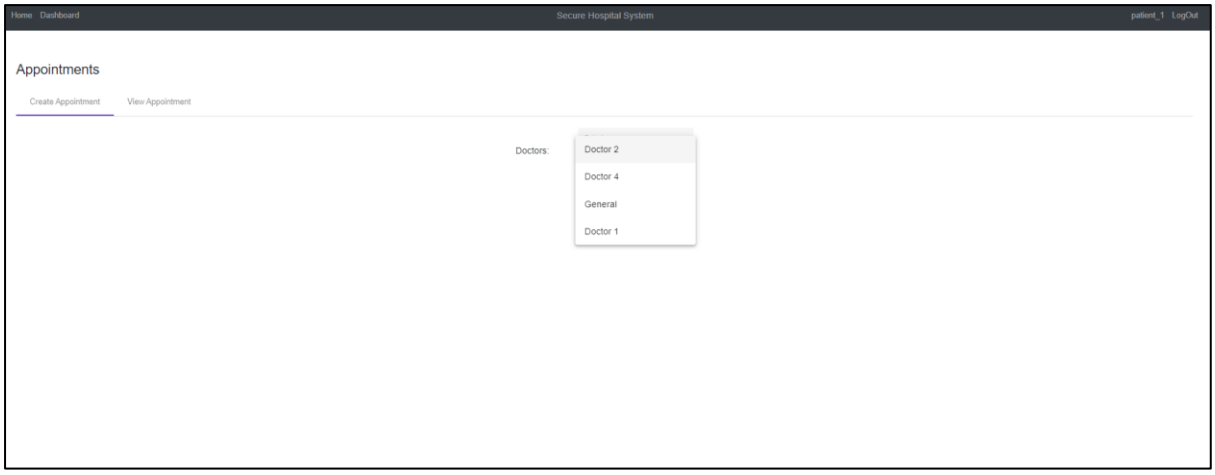
2.1 User: Patient

Login to the SHS webpage with the user role as patient. Below is the functionality and navigation through the patient user.

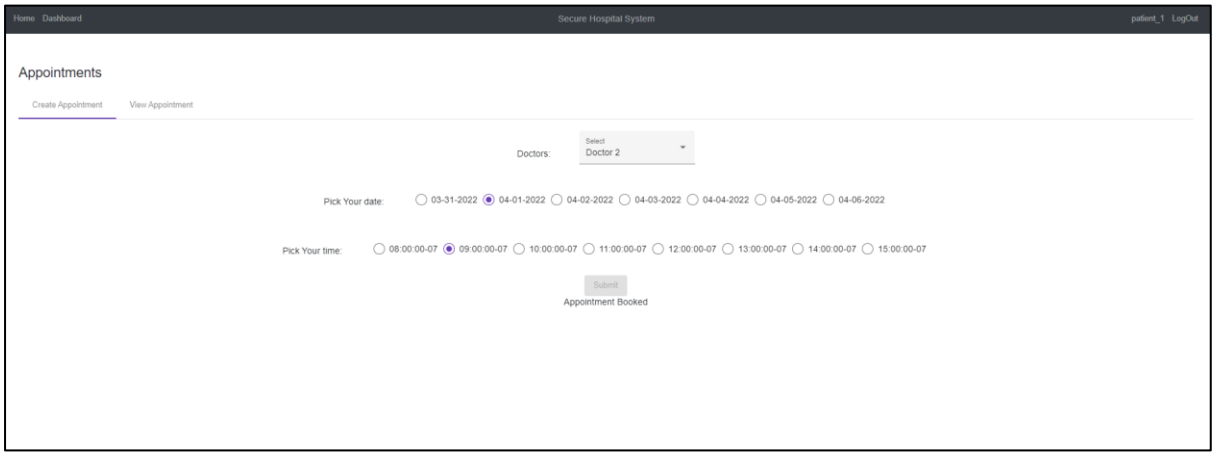
1. After logging in the patient can see the following dashboard for the patient along with patient name on the top:



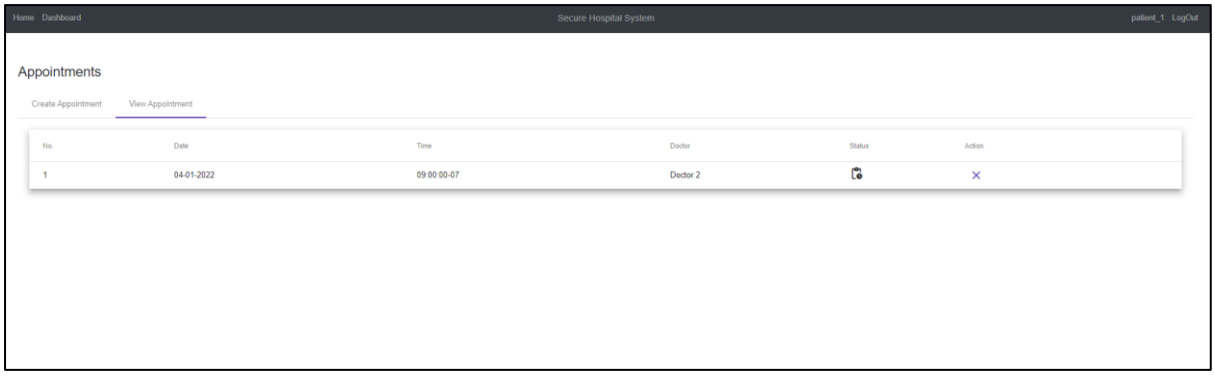
2. Now, by clicking on the appointments tab the patient can book the appointment with the doctor and the next page demonstrates how we can book an appointment with the doctor



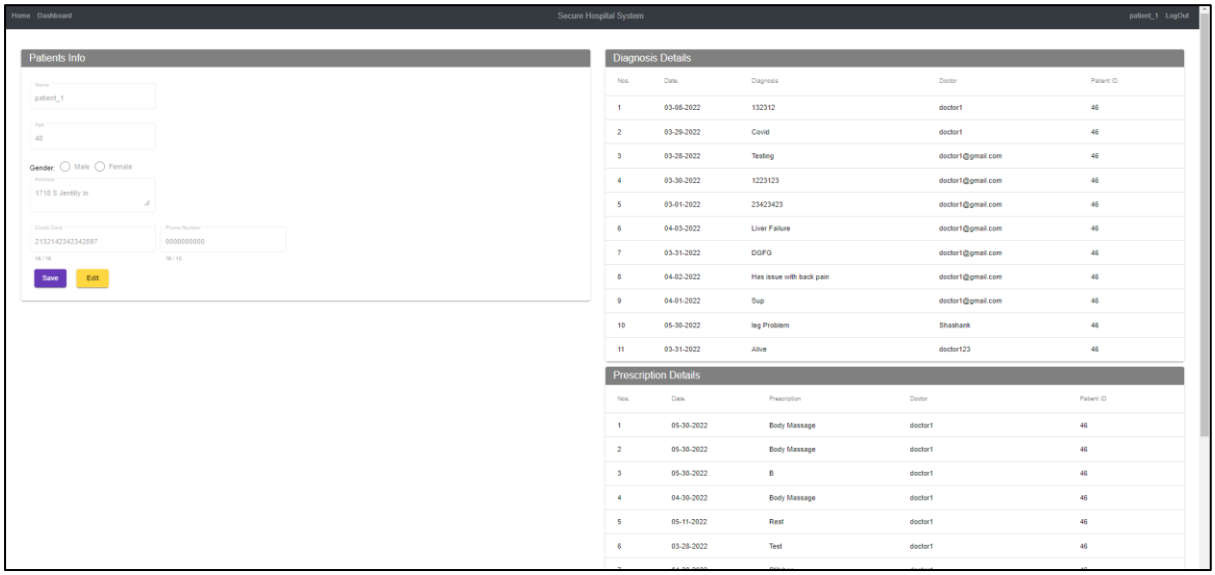
3. Once the patient selects the doctor, we display all the available time and slots for the given patient. After which the patient can click on Submit to book an appointment. Once it's completed it gets a message saying appointment booked.

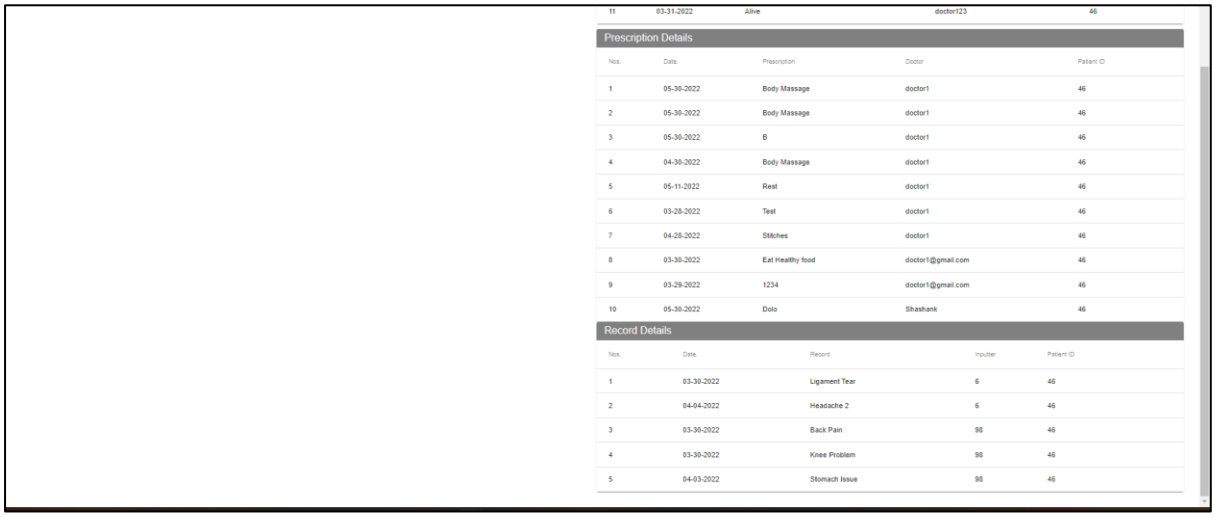


4. Also, after booking the appointment with doctor you can view your booked appointment on this page along with the status of your booked appointment by clicking on View appointment. Here the patient can also delete the booked appointment. Once the hospital staff approves the appointment the status changes and gets updated.

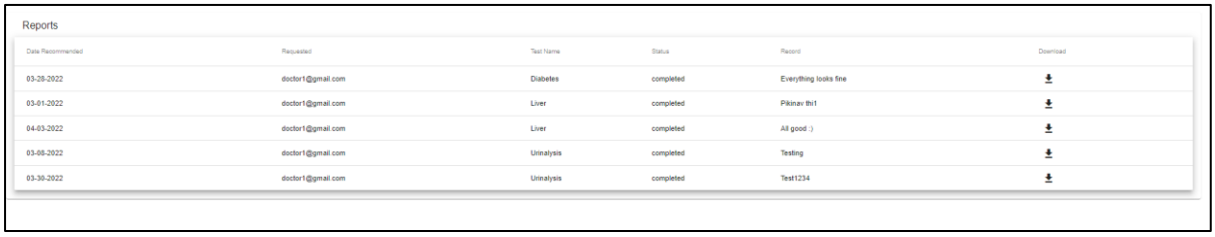


5. Now, the patient can go back on the Dashboard and click on any of the User Profile, Diagnosis, Prescription and Records. It will display the profile of the patient as well as its diagnosis details of any previous appointment as well as the prescription and record of the patient can be found on this page as given below:

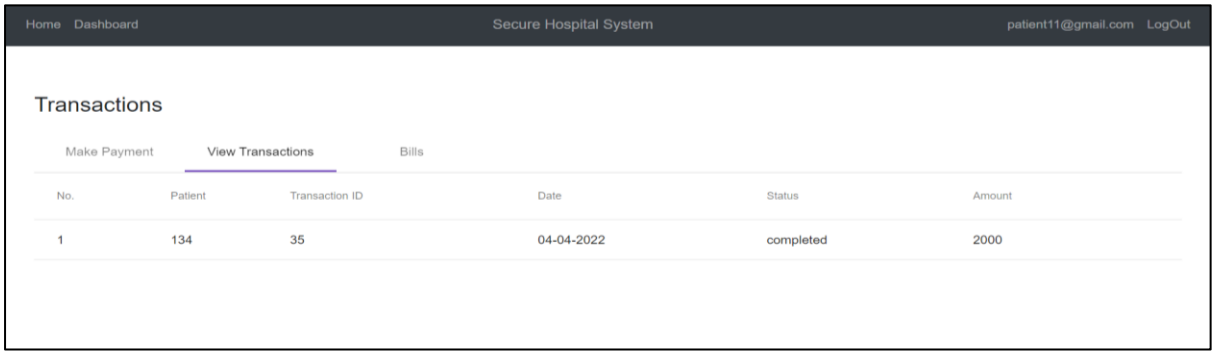




6. Now, the report of the tests for the patient can be found on the page given below. Also, the patient can download the lab report in the form of the pdf as given below:

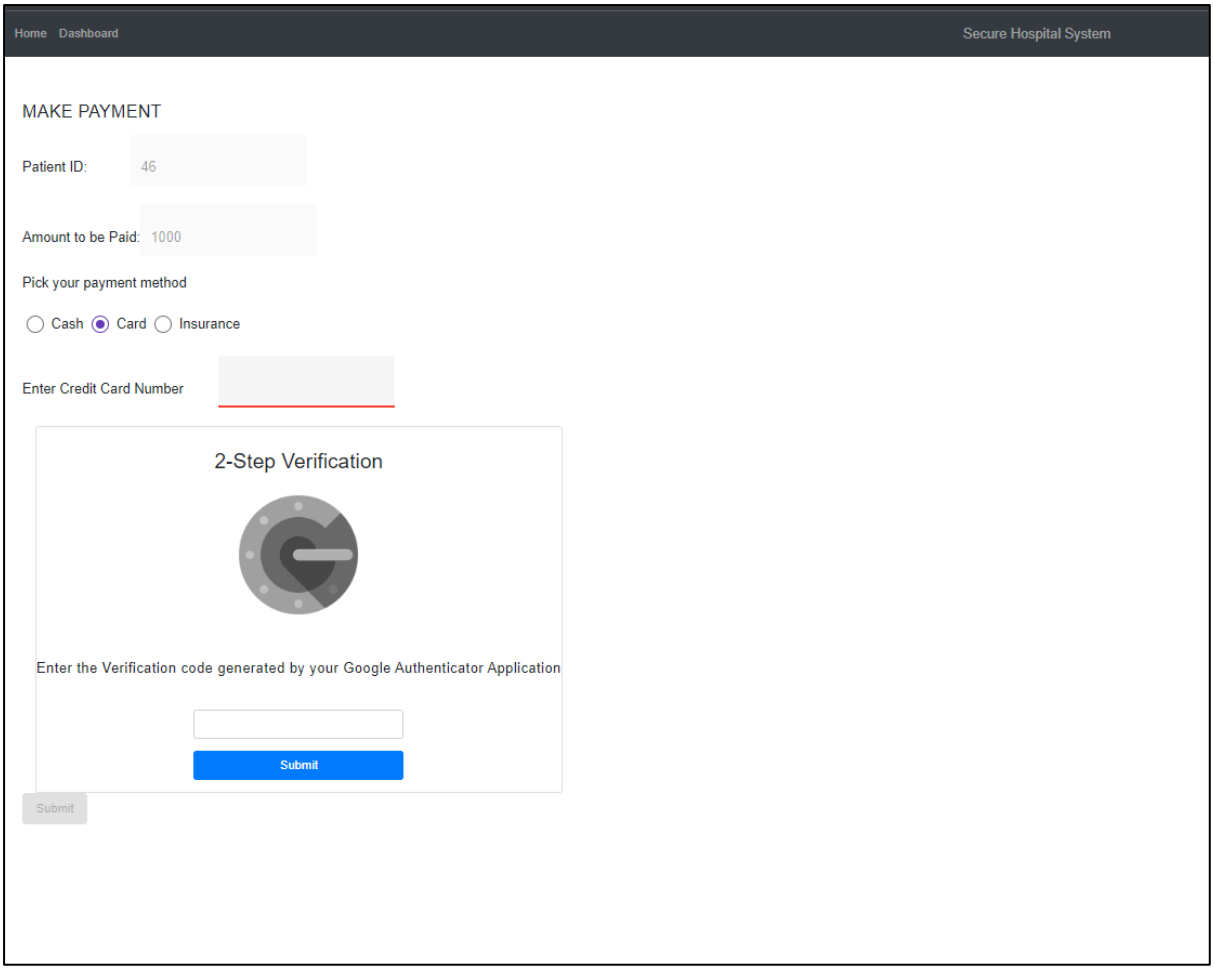


7. Now the bills of the patient can be downloaded on this page as it has tabs to see what transactions are being performed by the patient and also the past payment made by the patient. Also, the status of the transaction and the amount is also given on this page.

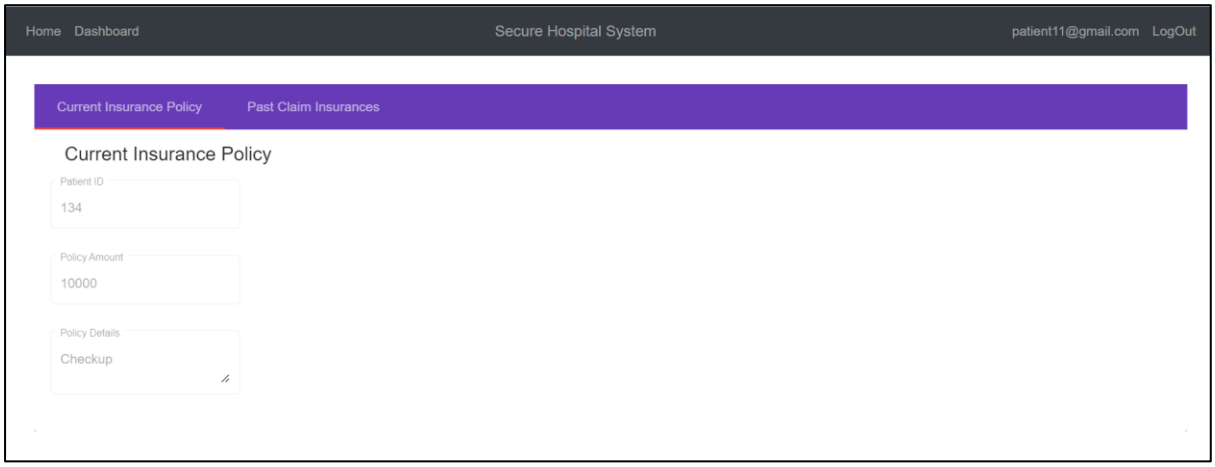


8. User can also make payment for the given amount by clicking the payment icon

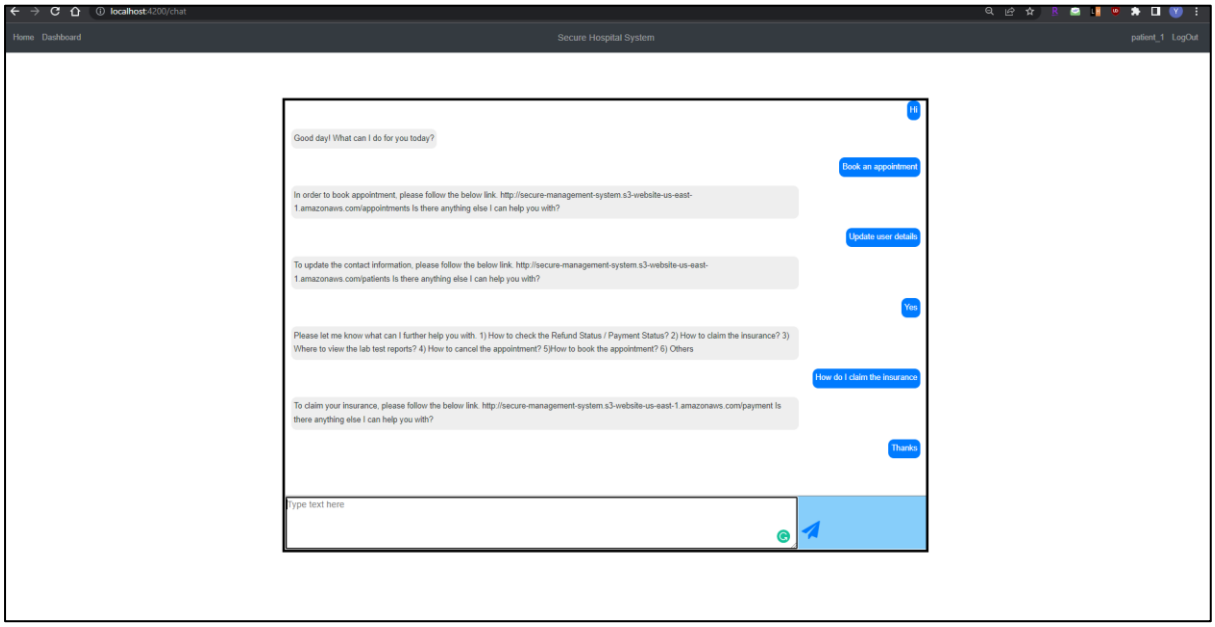
9. After the clicking the payment link it redirects to payment page where they can pay using cash, card, and insurance. After which the transaction table would be updated it, the transaction is completed.



10. Now, the given below page shows the insurances claimed by the patient as well as current insurance policy of the patient.



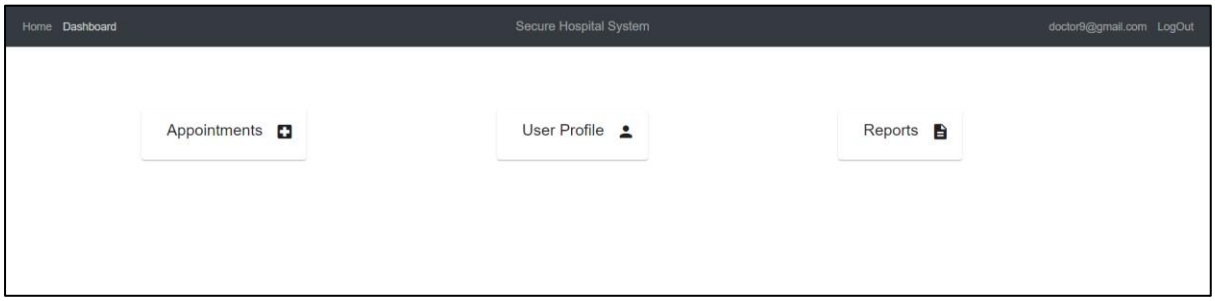
11. Now this page shows the chat bot which would help the user in getting the information it needs from the application.



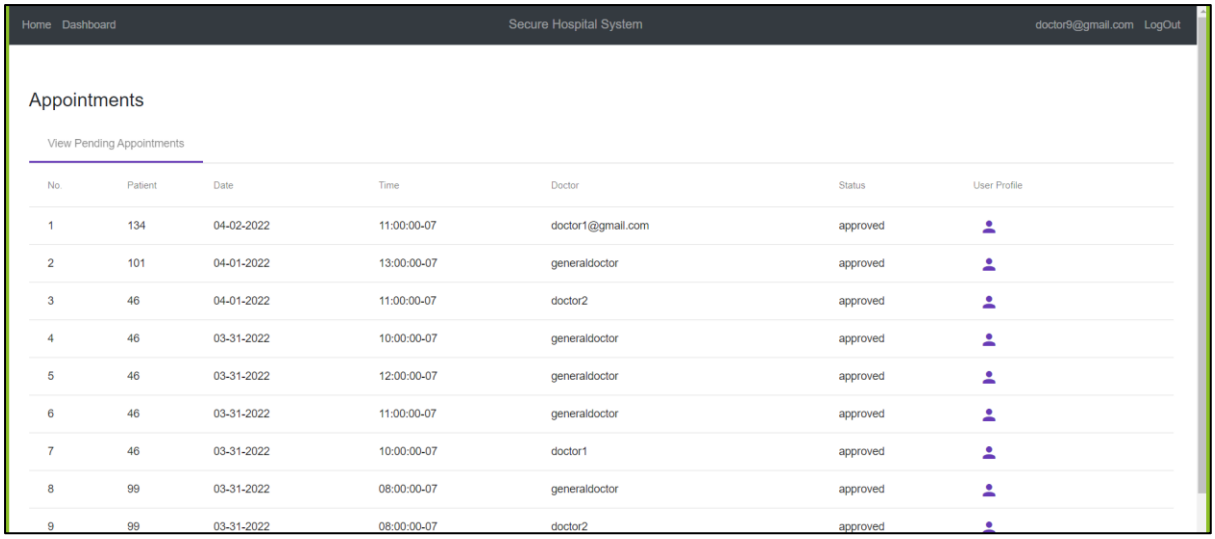
2.2 User: Doctor

Login to the SHS webpage with the user role as doctor. Below is the functionality and navigation through the doctor user.

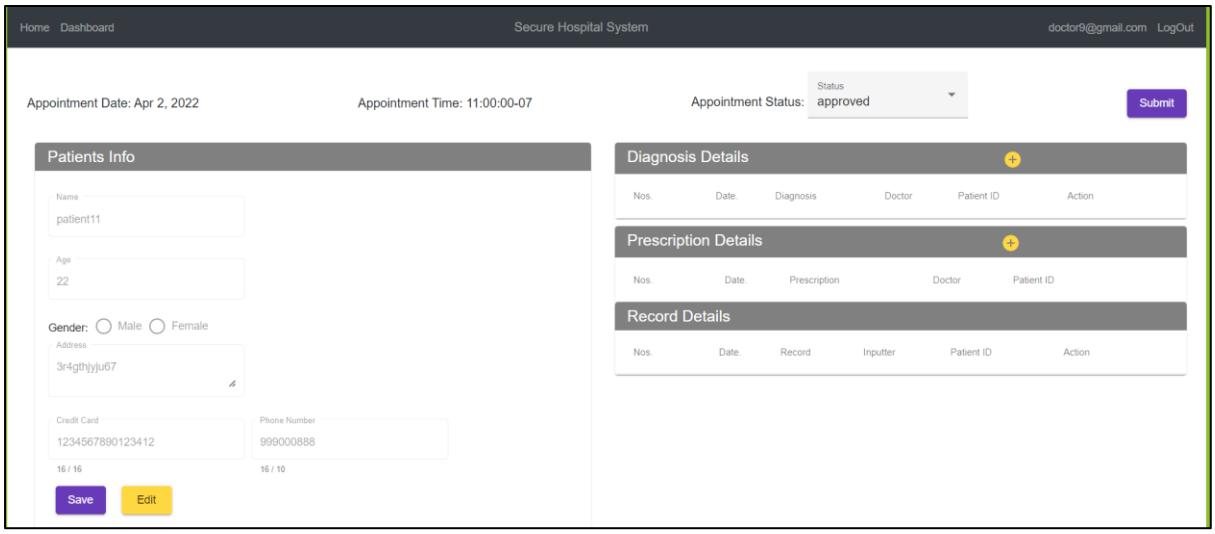
1. After logging in, the doctor will be able to see this dashboard:



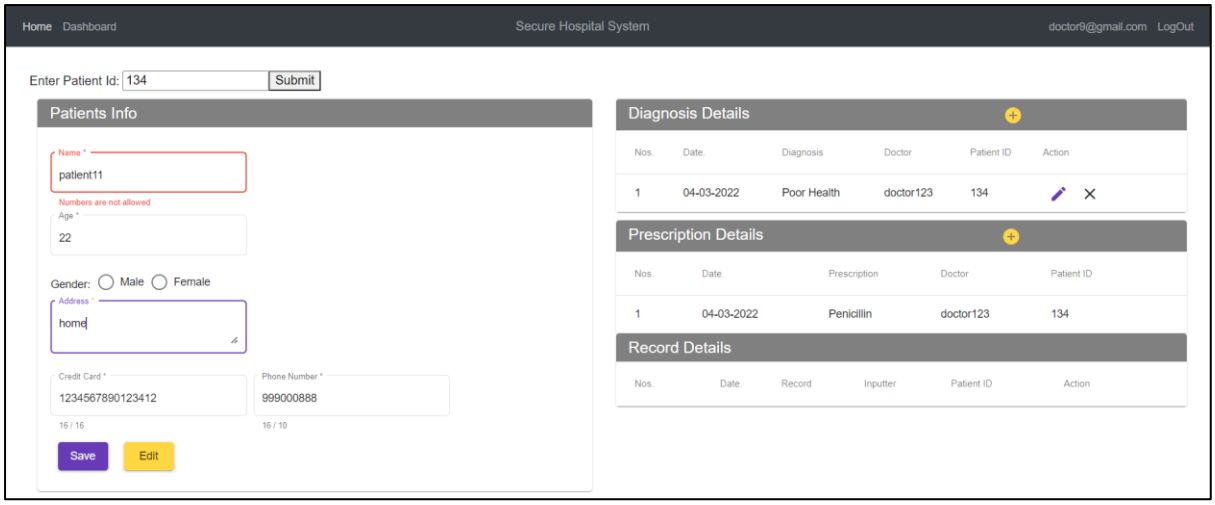
2. Doctors can click on appointments to see their approved appointments.



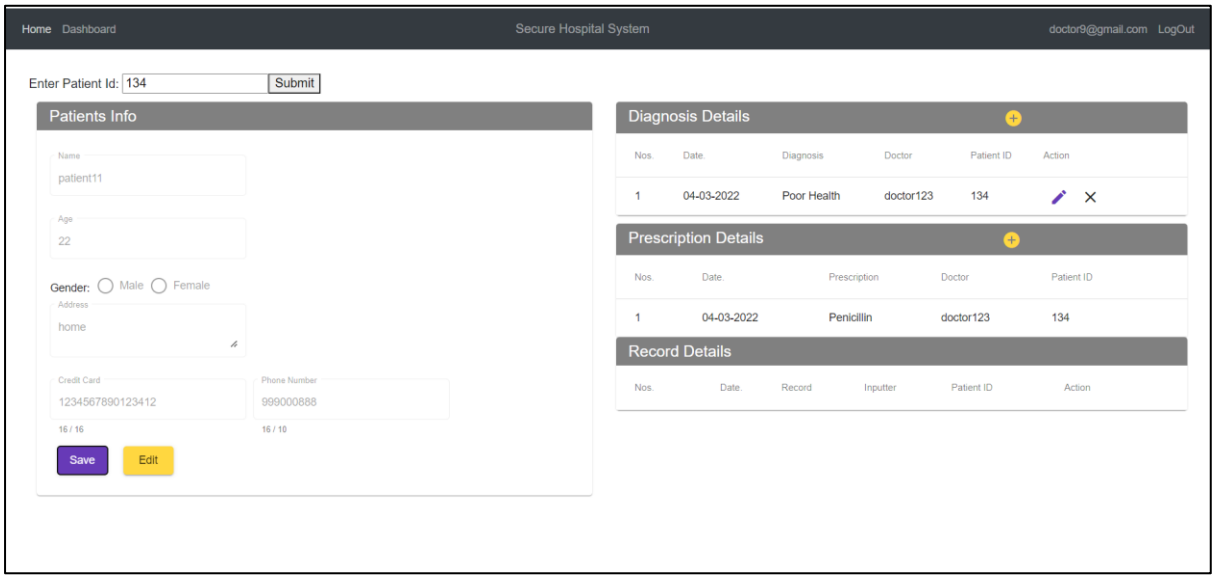
3. They can check the patient data of the patients who have approved appointments by clicking on the user profile button. They need to update the appointment status to complete the appointment and click submit button.



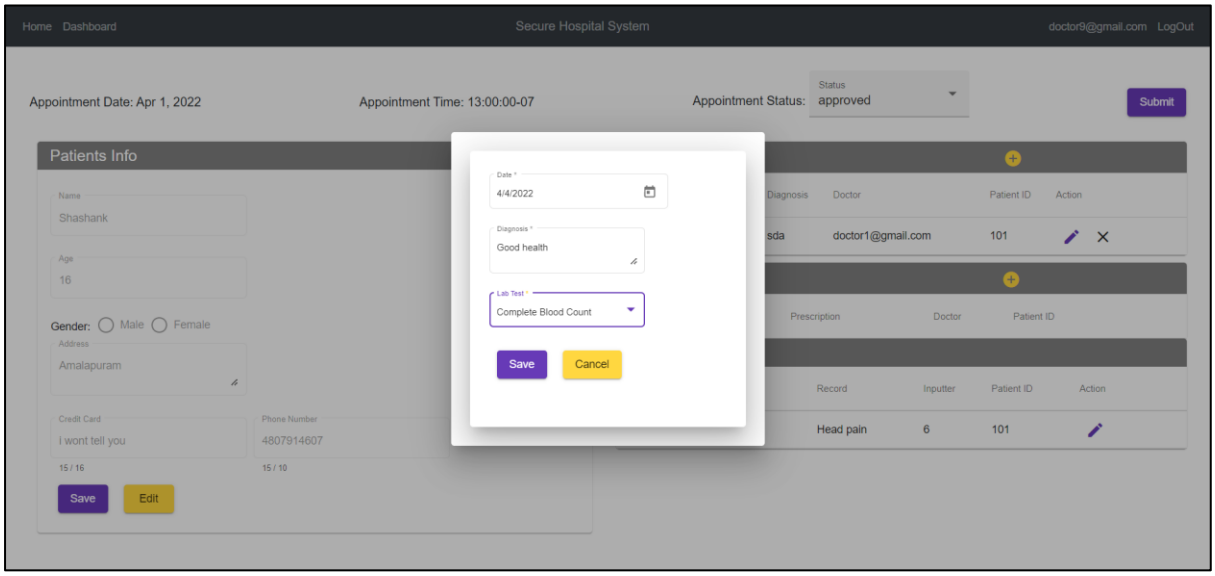
4. Doctor can edit the patient data.



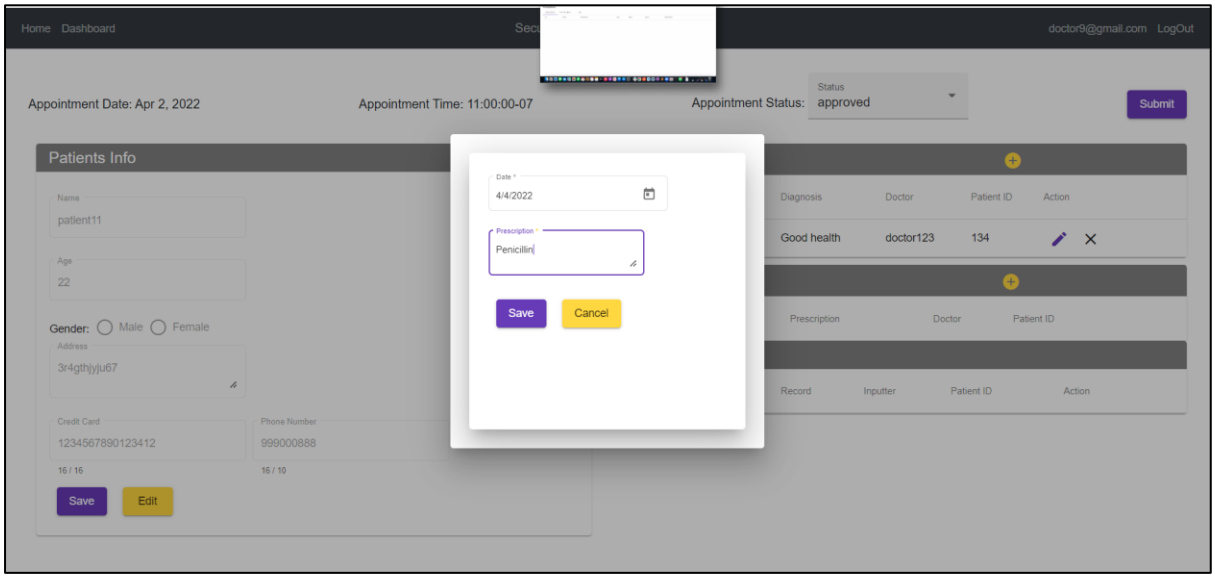
Below is the post update view.



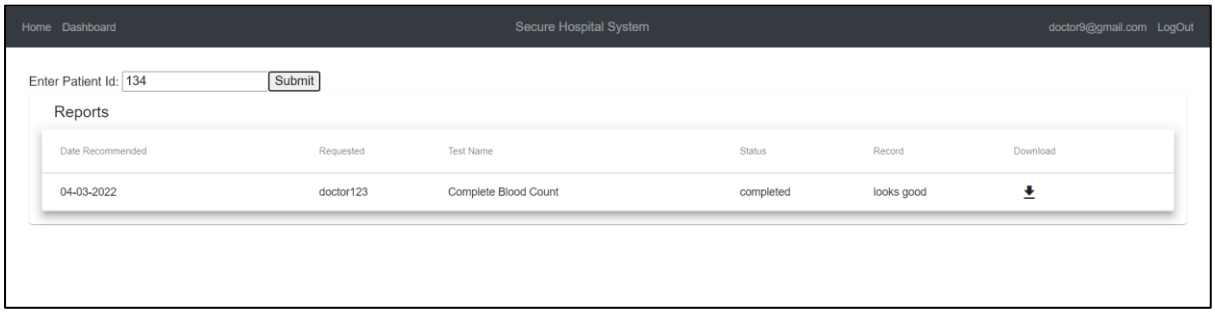
5. They can add and edit diagnoses and request lab tests.



6. They can prescribe medicine.



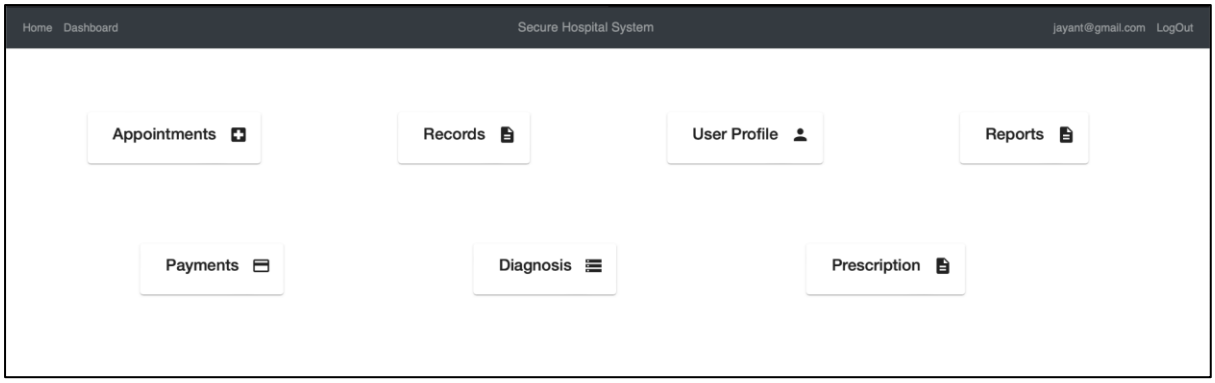
7. They can view lab test reports of the patient with the patient ID.



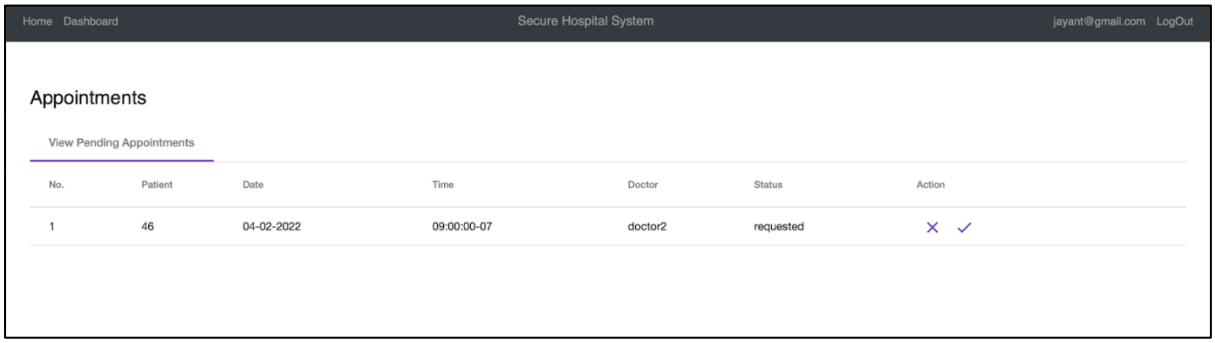
2.3 User: Hospital Staff

Login to the SHS webpage with the user role as hospital staff. Below is the functionality and navigation through the hospital staff user.

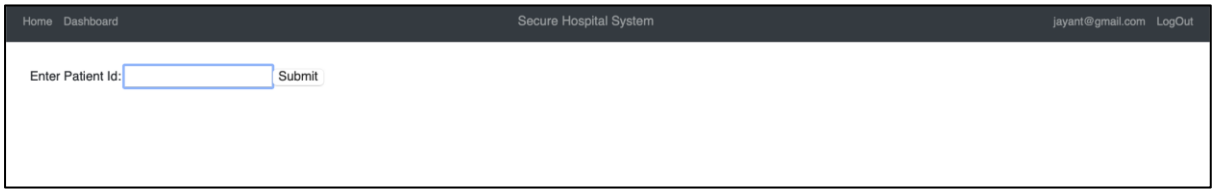
1. After logging in the hospital staff can see the following dashboard:



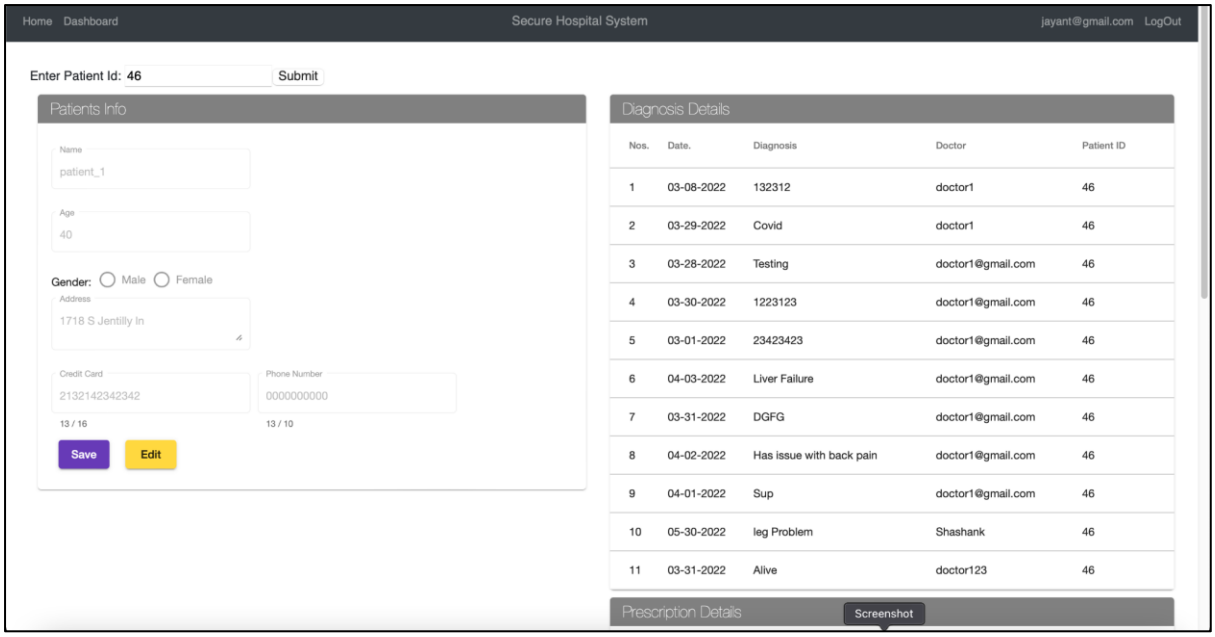
2. Now, by clicking on the appointments tab, hospital staff can review the appointments that were booked by the patients and approve them depending upon the priority and availability of the doctor.



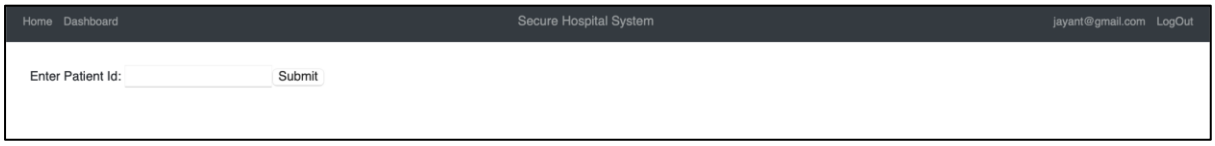
3. Now, we have a records section which requires the patient id to check or add information of a patient.



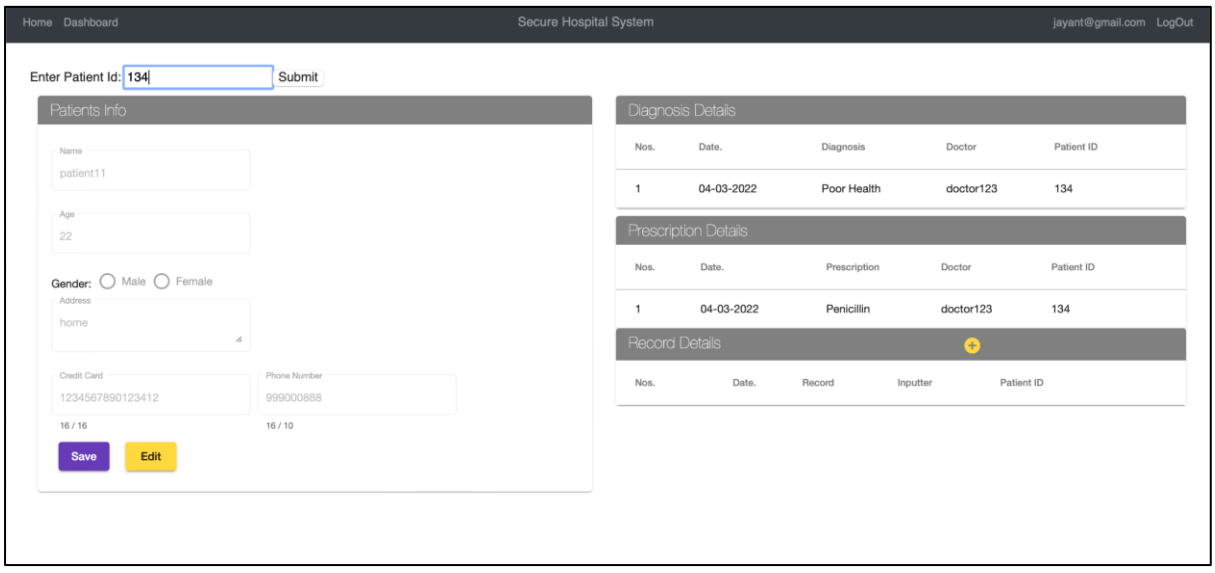
4. After the patient id is given, the hospital staff will have the option to add and update the patient details. They have the option to view the diagnosis, prescription and record details and the hospital staff will have the option to add the record details. All of the above 3 features have the same webpage to make the required changes.



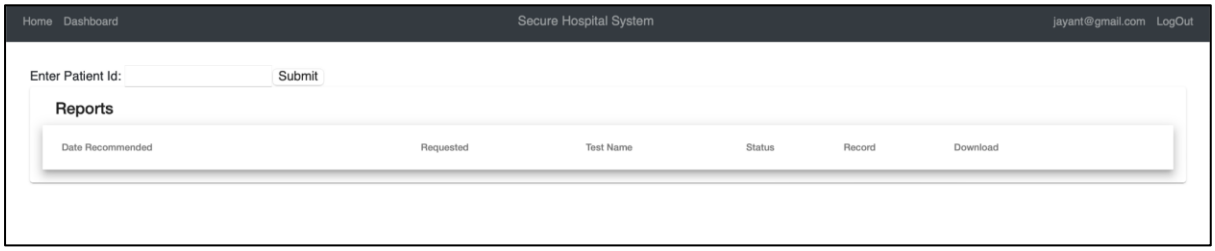
5. In the user profile section of the hospital staff, we will be asked the patient id to have the option to update the patient's personal info upon the request of the patient.



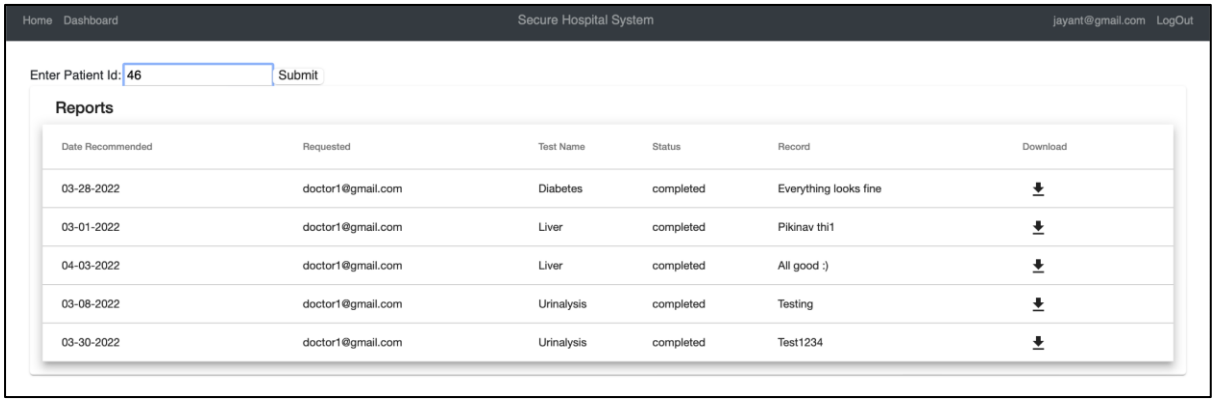
6. This page will help us to update the data of the patient upon their request.



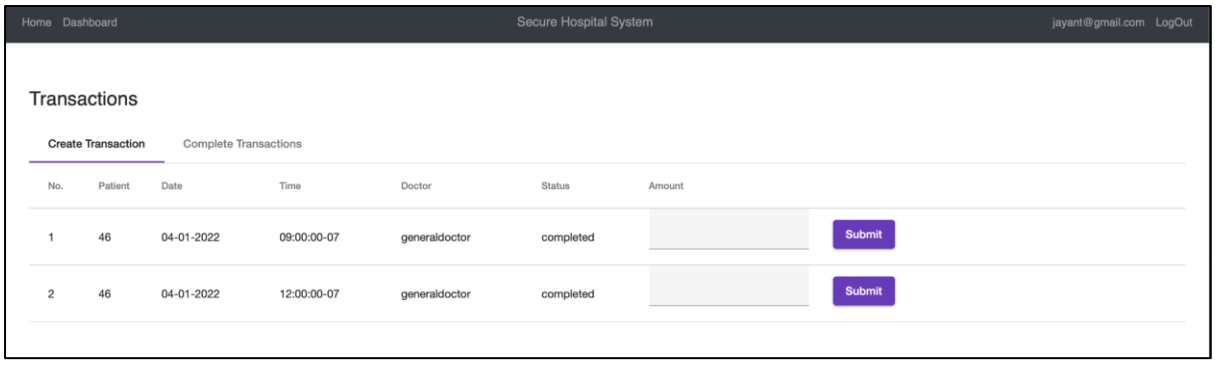
7. Then there is a reports tab which helps to see the reports of the patient after entering the patient id.



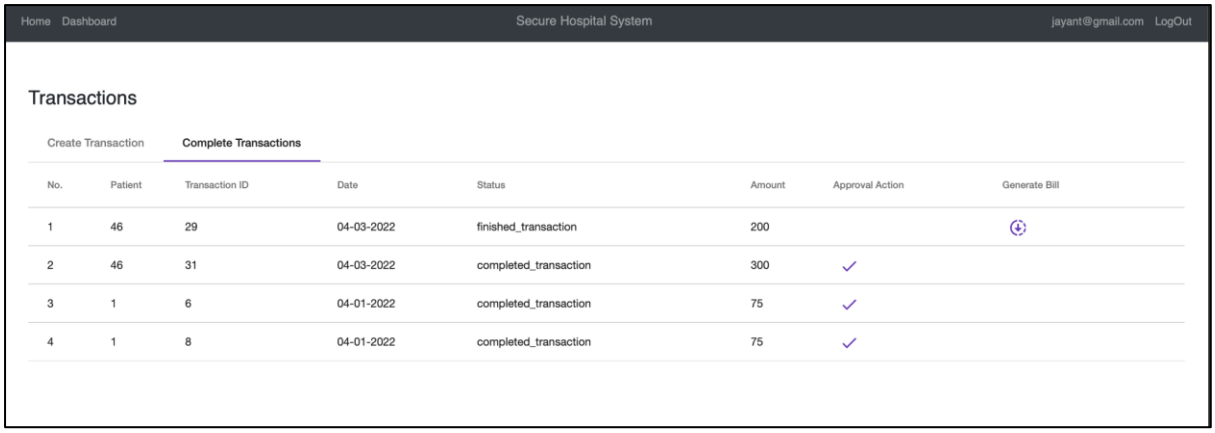
Down below is the screenshot which shows different reports concerning a patient id



8. Now, we have a payment tab where we have two options: create transaction and complete transaction. First, we can see the create transaction tab. Here, if the appointment with a doctor is confirmed, we can add the respective fee to consult the doctor and submit the transaction request.



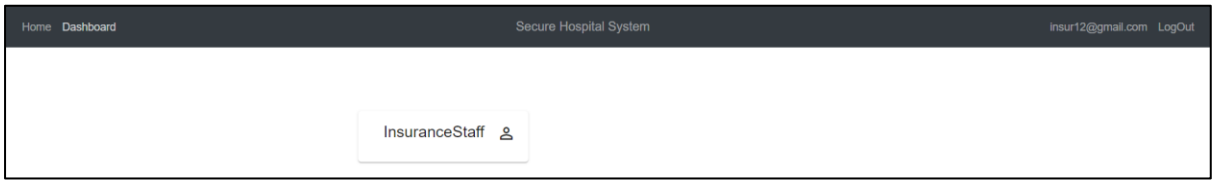
9. Now, we can look at the second tab which is the complete transaction. Here we have the option to complete the transaction upon approval of the appointment with the doctor. The bill is generated, and we will have the option to download and print the bill upon the request of the patient.



2.4 User: Insurance Staff

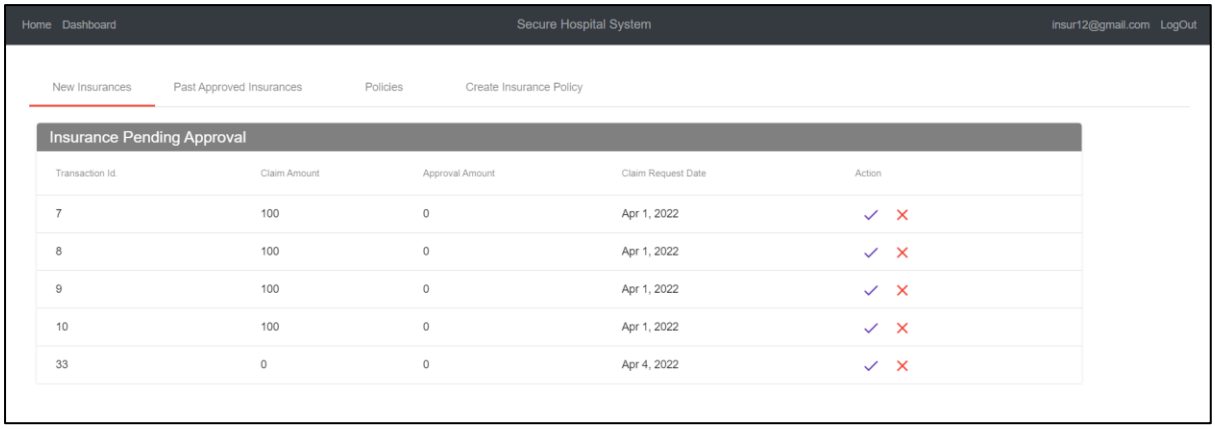
The insurance staff has the privileges to manage the Insurance Claims of the patients and also add individual Insurance Policies to any of the required patients. Insurance staff has the access to view, review and validate claim requests received from the patients. They can create new insurance policies and insurance records of patients whenever necessary. They have the power to review the insurance claims and approve/deny any insurance claim.

1. Once logged in as an Insurance Staff member, the staff member has his individual Staff bar in the dashboard, where he can perform all of his activities related to Insurance Claims and Policies.

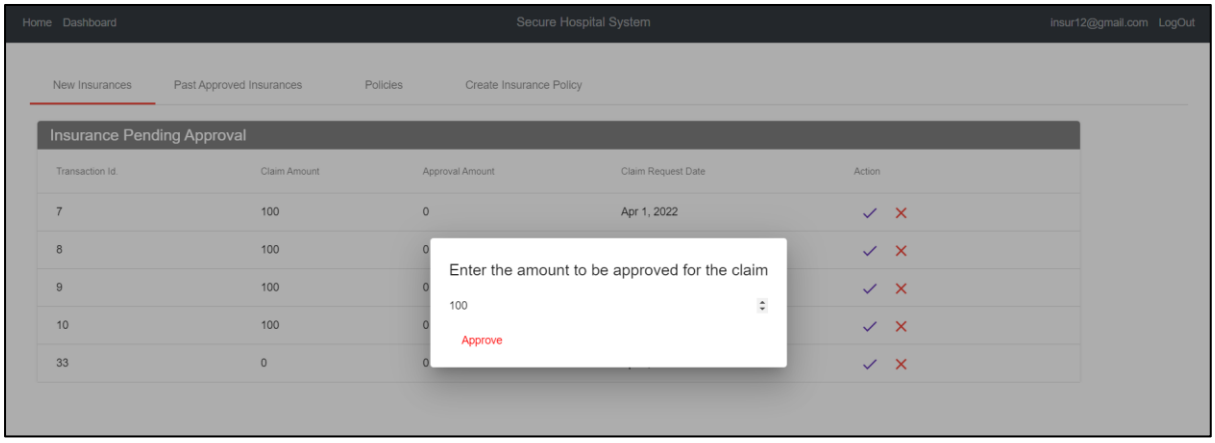


2. Once he selects the Insurance Staff Bar, they get to choose from the list of tasks they want to perform, such as reviewing new Claims, and also the ability to create new insurance policies.

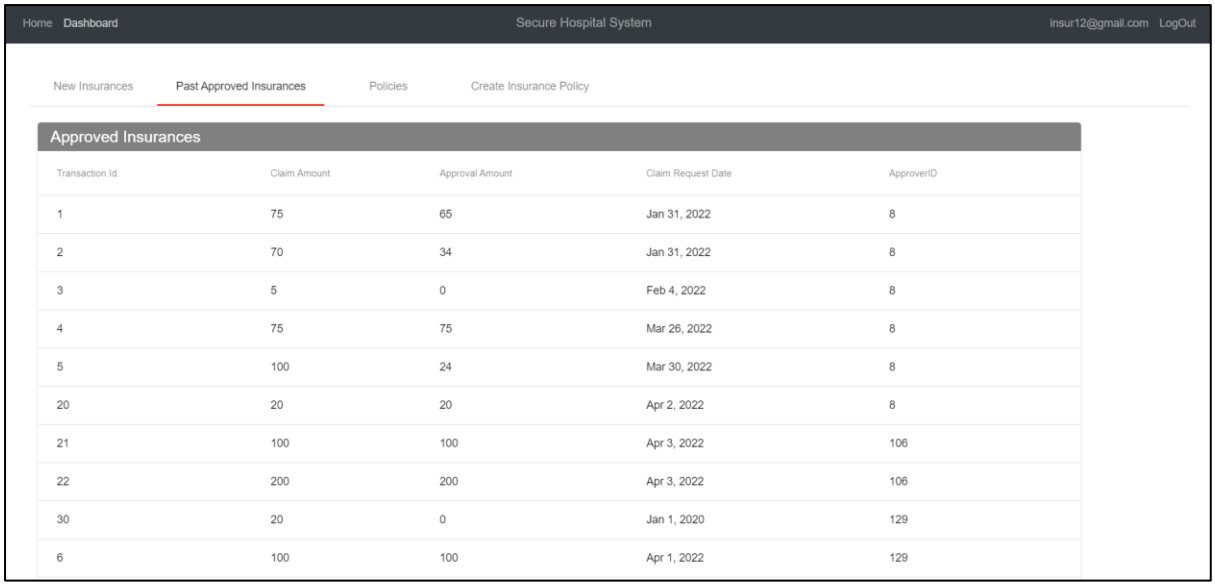
   Under the New Insurances section, they will have all the list of Insurance Claims that have been requested by various patients. The staff will be able to review and verify the Claims requested by the patients. If the staff chooses to deny the request of a particular claim, they can just click on the corresponding ‘X’ remove it from the list.



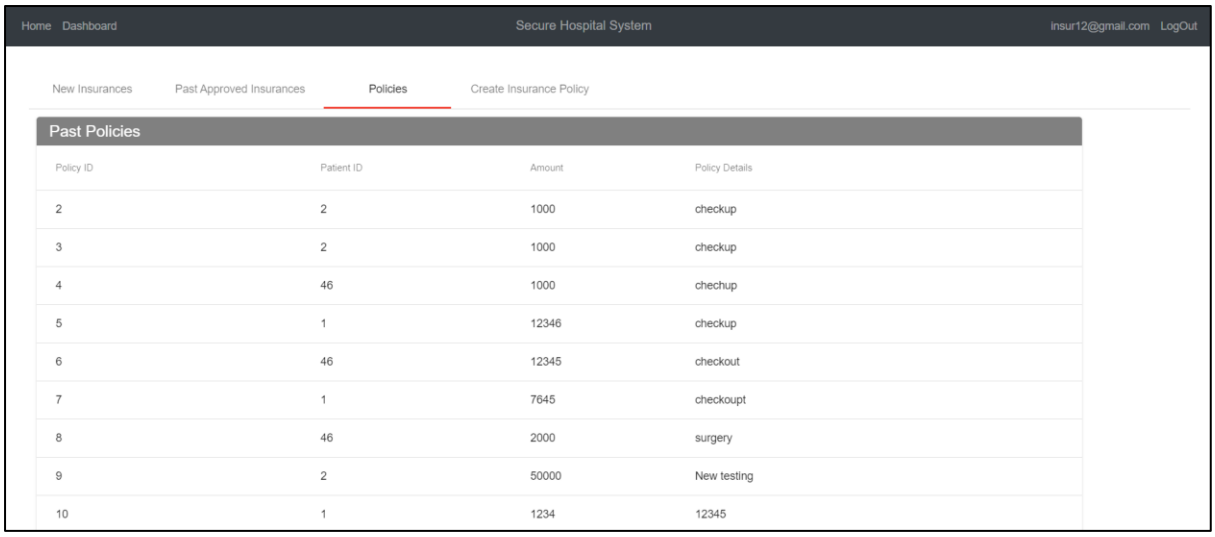
3. If the insurance staff choose to approve a particular request, they just need to click on the ‘Tick’ and a new window pops up where they can enter the amount they wish to approve.



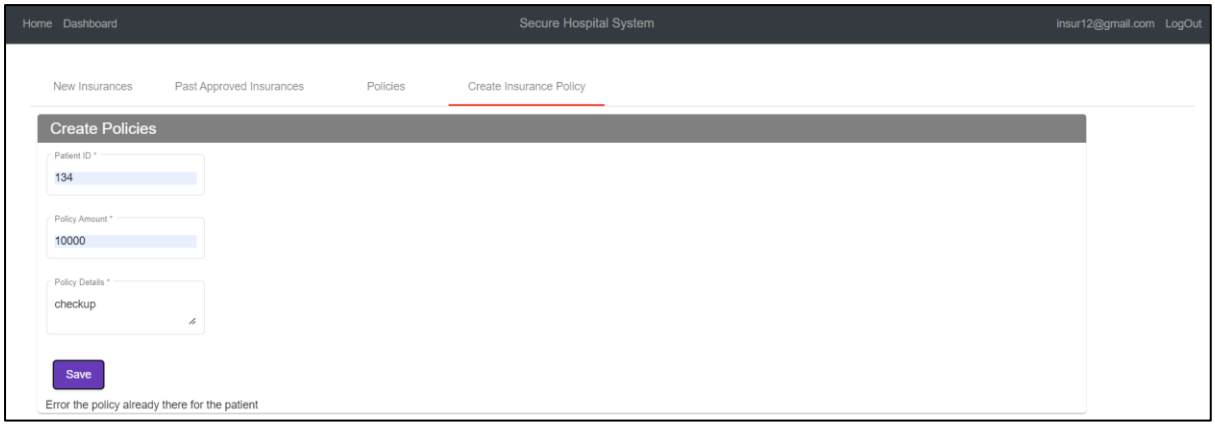
4. On approval of insurance claims, it will be moved to the Past Approved Insurances, where they will be able to access the record of all the approved insurance claims. Once the insurance staff approves/denies an insurance request, it gets reflected in the patient profile as well, so that the patient will be able to view the status of their insurance claims.



5. The Policies section contains all the records of the insurance policies associated with the patients. This lets the insurance staff an estimate of how much amount they can approve for an insurance claim.



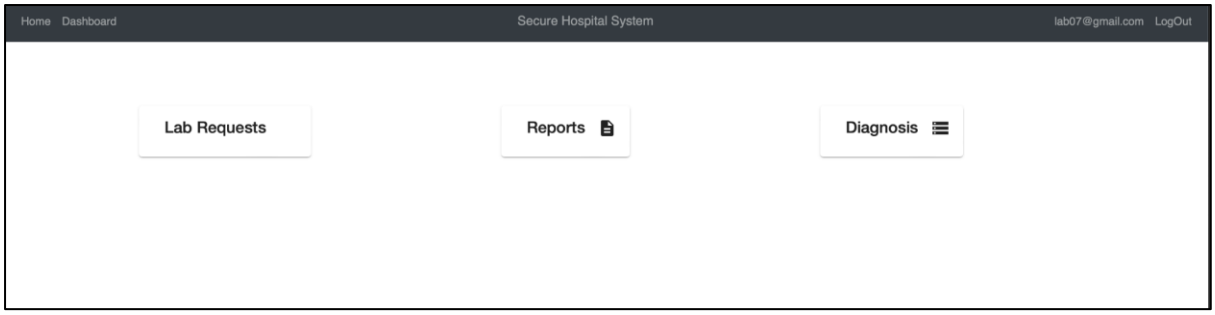
6. Under the Create Insurance Policy section, the staff will be able to create new insurance policies for patients based on their requirements and eligibility.



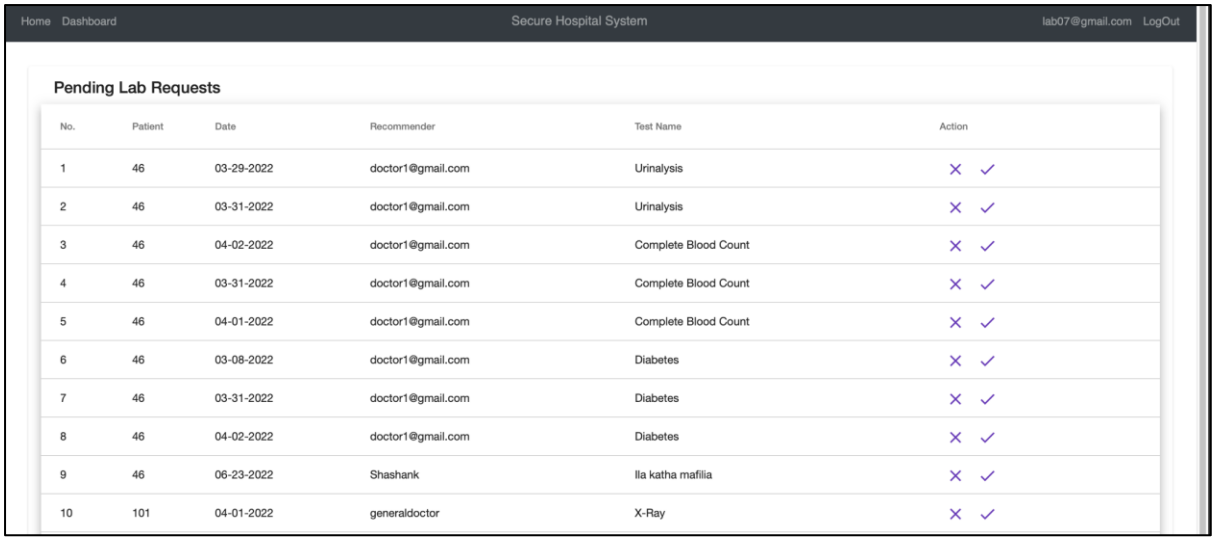
2.5 User: Lab Staff

Login to the SHS webpage with the user role as lab staff. Below is the functionality and navigation through the lab staff user.

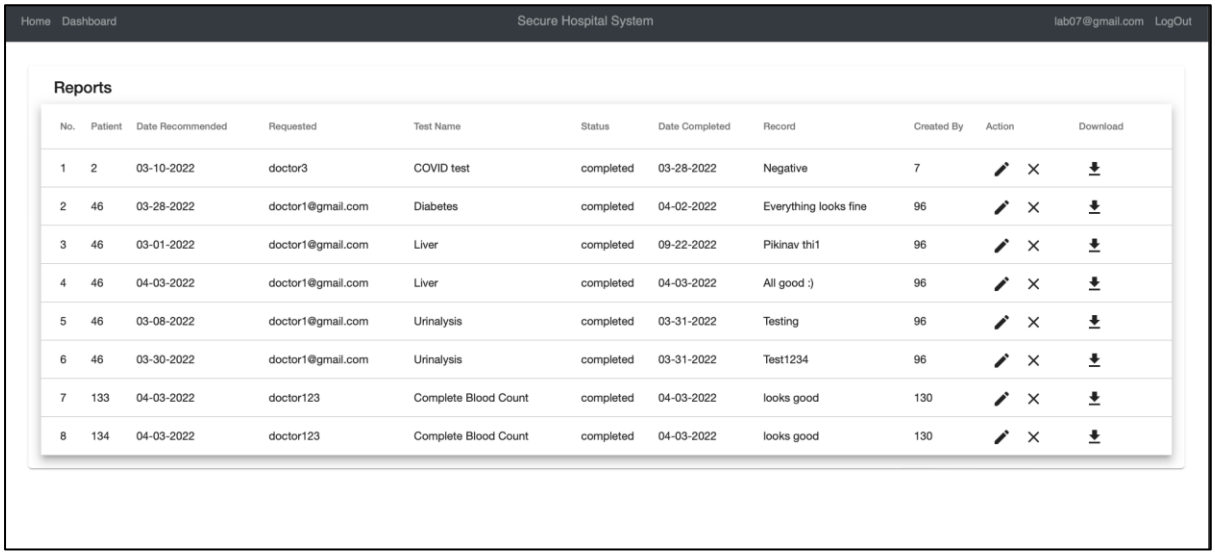
1. After logging in as a lab staff, this is the dashboard the lab staff will have access to:



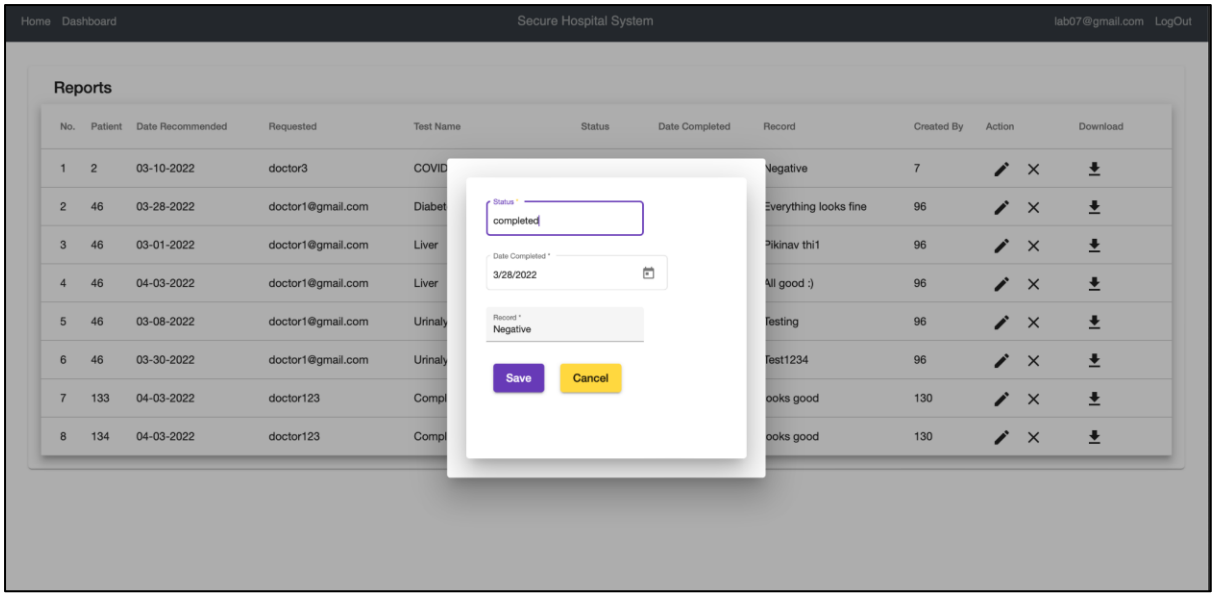
2. After going into the lab requests, we can see all the pending lab requests that were requested by the doctor. Now, the lab staff will have the option to approve those requests they get from the doctors for patients.



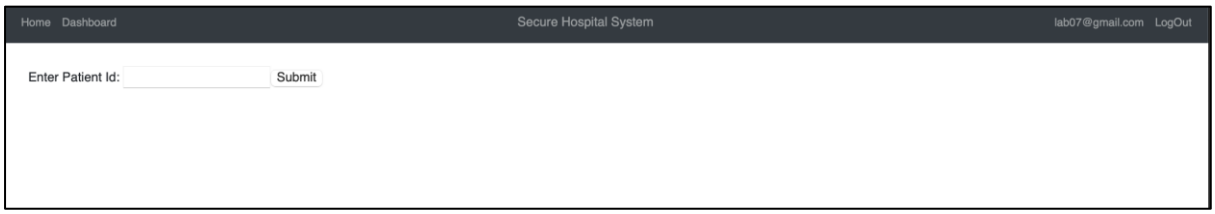
3. After the lab staff approves the pending requests, it is moved to the report section of the lab staff, where the lab staff have to fill in the details depending on the status of the lab test that is performed. Down below is the report section of the lab staff where they can edit and update the status of the test. Once the report is finalized, the lab staff will have the option to download the report.



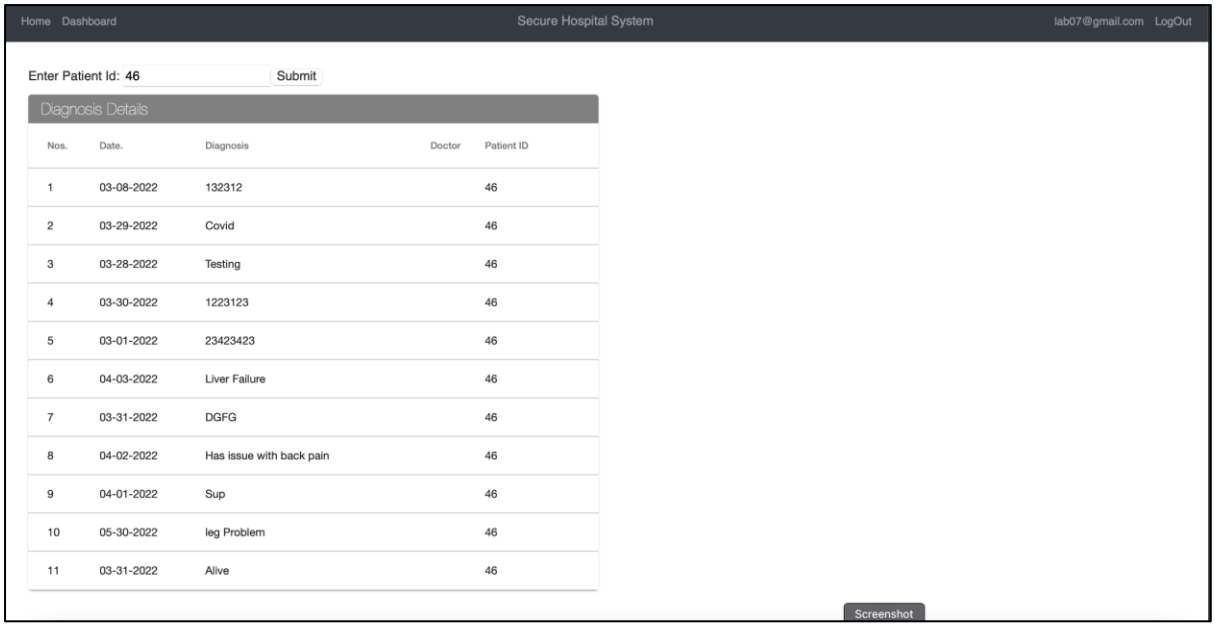
4. In the action bar of the report, we have three sections which is status, date and the record which can be edited by the lab staff whenever possible.



5. Another functionality of the lab staff is diagnosis, where the lab staff has the option to view the patient diagnosis. After, clicking the diagnosis tab in the dashboard we will be asked for a patient id.



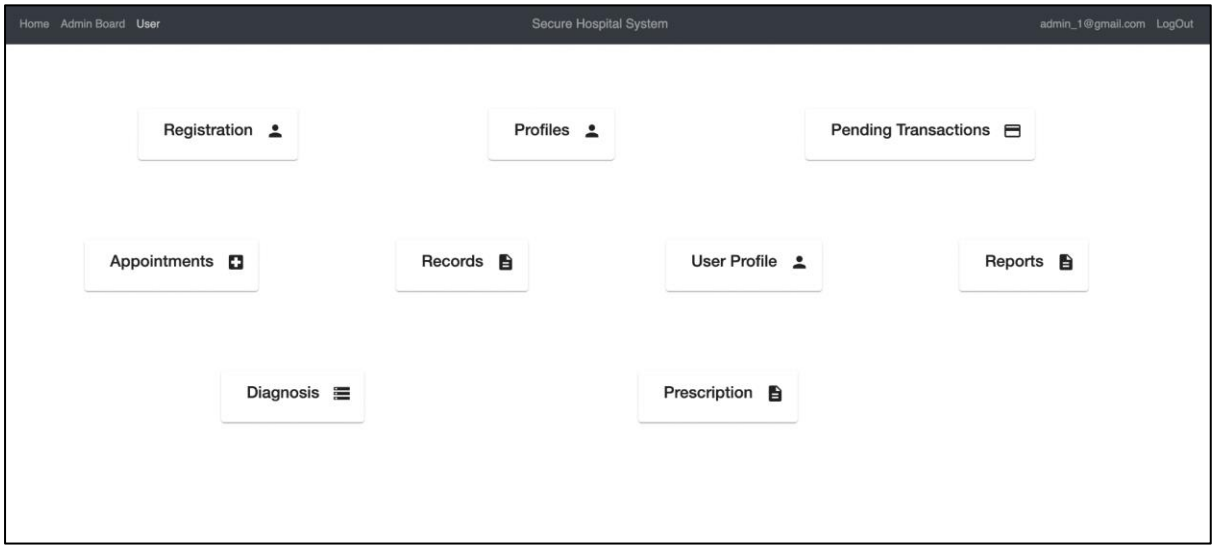
6. After entering the patient id, the diagnosis data of the patient given by the doctor is available for the lab staff for viewing.



2.6 User: Admin

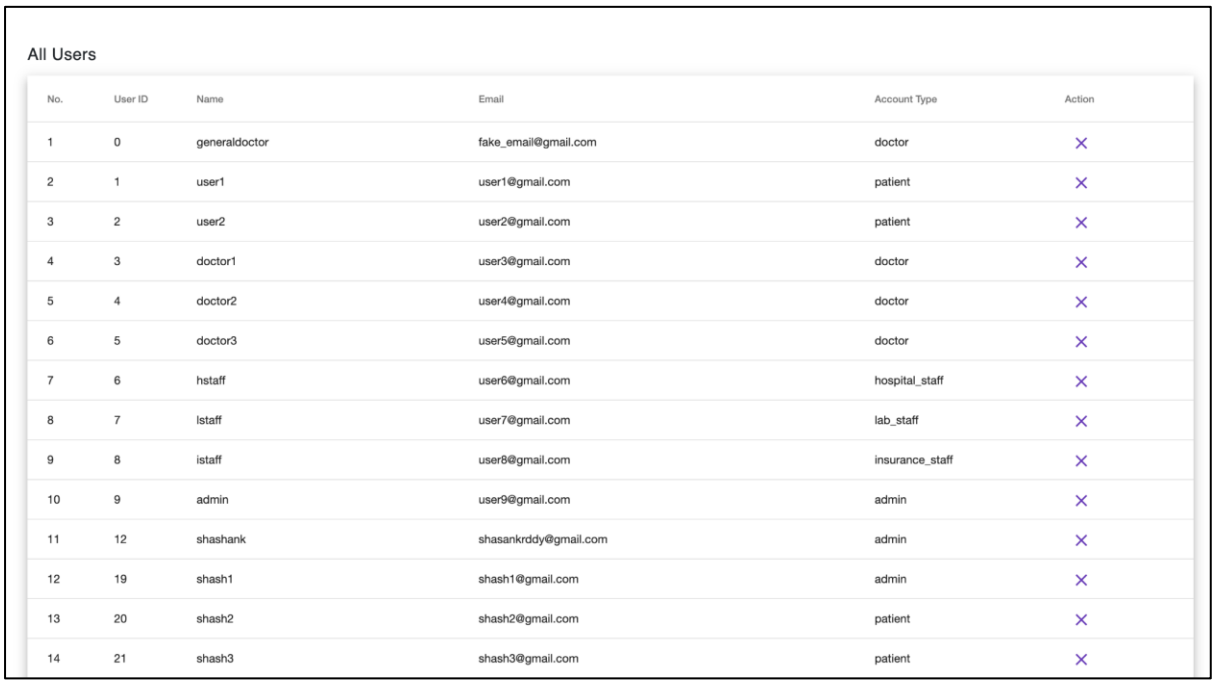
The administrator role has all the highest privileges on the application, as he can create, edit, and delete any records, must authorize transactions, and has access to all log files. The admin is responsible for the smooth functioning of the hospital system.

1. After logging in to his profile a dashboard as below is displayed, where he can navigate to the respective pages.



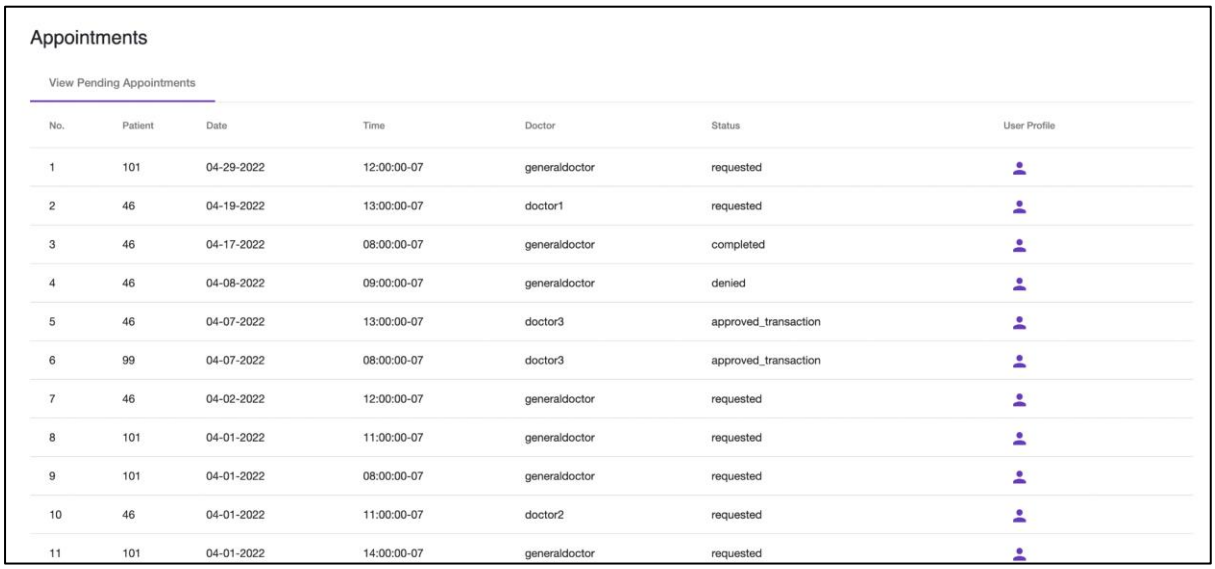
2. When the admin navigates to the “Registration” page, he will be able to register a employees of the hospital like doctor, lab staff, insurance staff, hospital staff by providing their details

3. Admin can edit the profiles of the employees by navigating to the profiles page

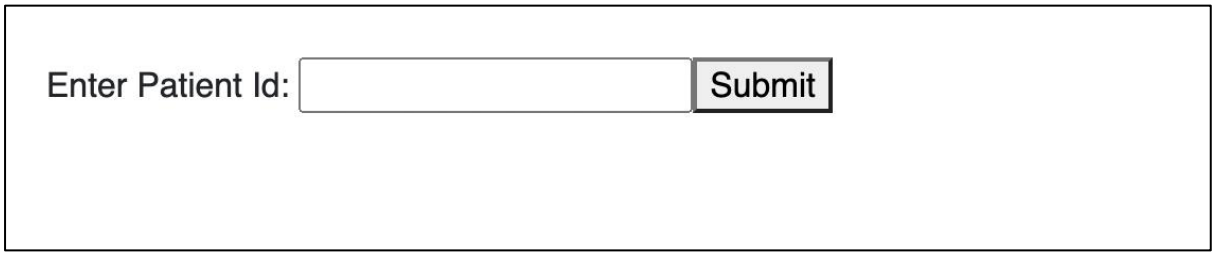


4. Admin should approve transactions by navigating to the transactions page

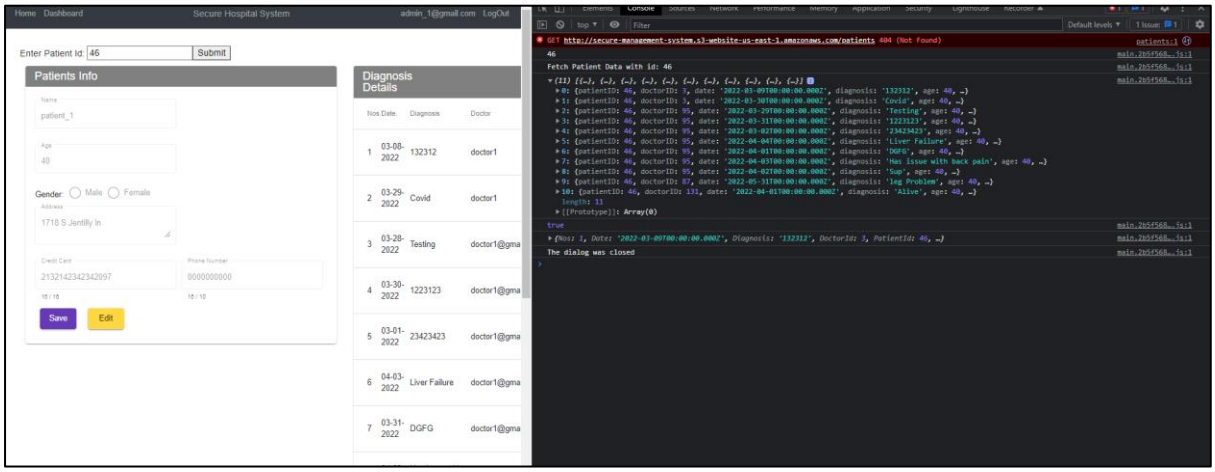
5. The admin can take action on appointments by navigating to the “appointments” page



6. The admin can access patient profiles and update each of their prescriptions, diagnosis, and records by providing the patient’s id



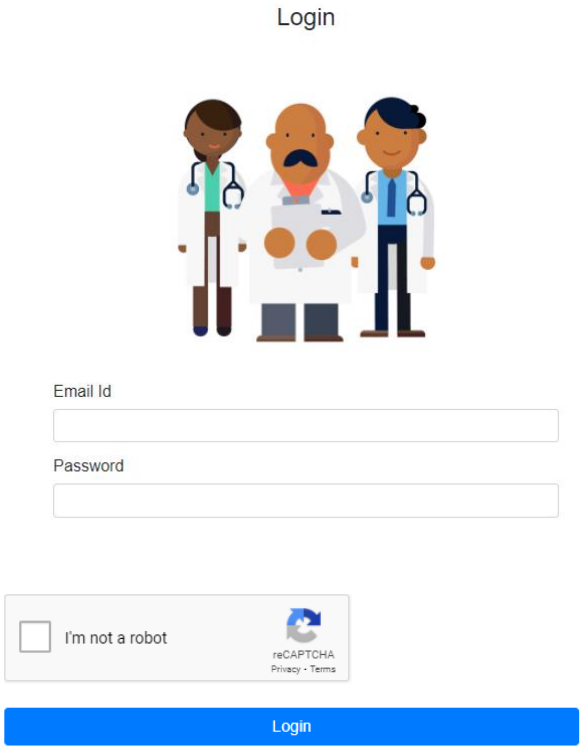
7. System Logs: Admin can access and view the system log files.

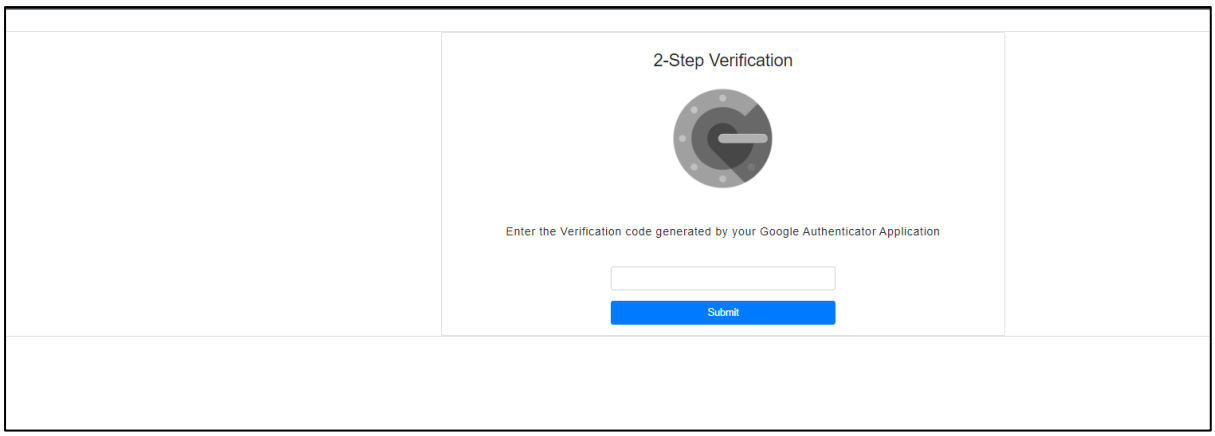


4. Security Workflow

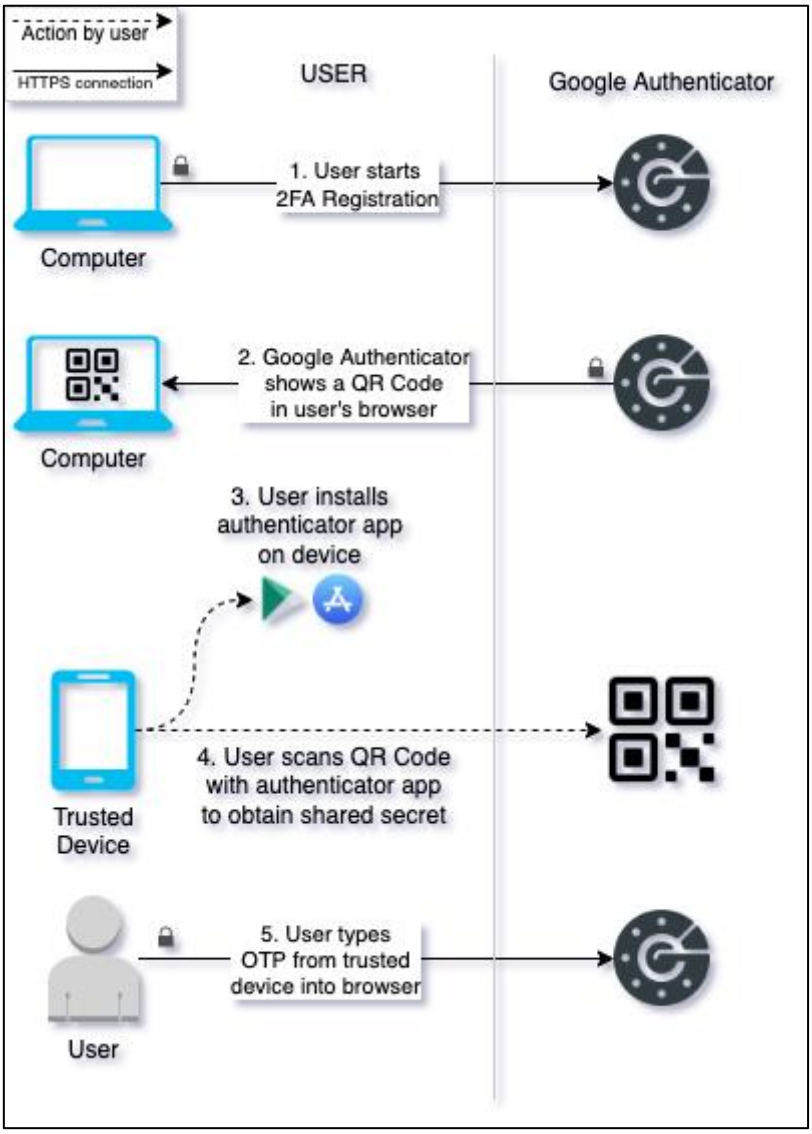
4.1 Login to SHS

Login page to for the secure hospital system.





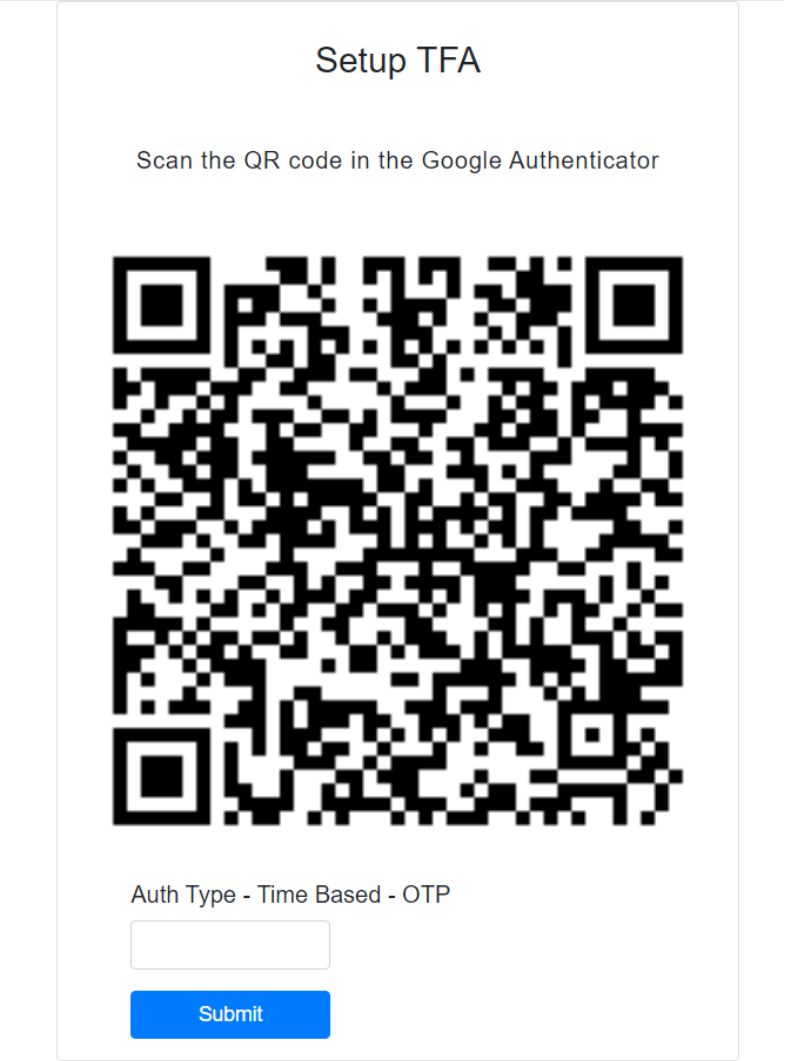
Below diagram describes the process flow of the user login authentication.



4.2 Setup 2FA

Setup the 2 Factor Authentication using Google Authenticator for secure Login.

1. Install the Authenticator app by Google from the Play Store (Android) or from the AppStore (IOS).
2. We need to link the Website Login with the Google Authenticator during registration.
3. On the Registration page, once the user enters the details and clicks the Sign-Up Button, a unique QR code will be generated which is used to link the user with the Google Authenticator



Note*: This is a onetime generated QR Code, please make sure to scan it.

4. Now, scan the QR code using the Google Authenticator app. On scanning, the app starts to generate the new code every 30 seconds.

5. Enter the code within the timeframe into the website to initiate a secure login.