**Enumerated DiagnoGenie Requirements**

***1. Functionality Requirements***

***1.1 User Management***

**<DG-USER- 010>User Management**

The DG system shall be capable of managing users with various roles, including administrators, receptionists, lab assistants, lab technicians, supervisors, doctors, and patients.

**<end of DG-USER- 010>**

**<DG-USER- 020>User Registration**

The system shall offer a user registration form that patients can use to sign up online. The registration form shall collect relevant patient information such as name, date of birth, contact details, and medical history.

**<end of DG-USER- 020>**

**<DG-USER- 030>User Roles**

The system shall define different user roles, such as Administrator, Receptionist, Doctor, Lab assistant, Lab technician, Supervisor, and Patient.

**<end of DG-USER- 030>**

**<DG-USER- 040>User Account Creation**

The Administrator shall have the ability to create new user accounts for Receptionist, Lab Technician, Lab Assistant, Supervisor, and Doctor roles. Patient accounts shall be created automatically upon successful registration.

**<end of DG-USER- 040>**

**<DG-USER- 050>User Authentication**

The system shall provide a robust user authentication mechanism, such as a username and password combination, to verify the identity of users before granting access to the system.

**<end of DG-USER- 050>**

**<DG-USER- 060>User Permissions**

The system shall provide granular user permissions to control access to different parts of the system. For example, Receptionists shall have permissions to manage patient appointments, while Doctors shall have permissions to view and update patient medical records.

**<end of DG-USER- 060>**

**<DG-USER- 070>Session Token creation**

The system shall create a session token after authentication, which shall include the session data for continuing the session.

**<end of DG-USER- 070>**

**<DG-USER- 080>Error Handling**

The system shall throw an error if the user credentials do not match or if user already exists in the database.

**<end of DG-USER- 080>**

***1.2 Booking a test***

**<DG-BOOKING- 010>Login Functionality**

The system shall allow patients to log in to their account to book a test online. The login functionality shall provide a secure and authenticated interface for the patients to access their account.

**<end of DG-BOOKING- 010>**

**<DG-BOOKING- 020>Walk-In Registration**

The receptionist shall be able to register a patient who walks in to the laboratory. The registration process shall include collecting the patient's personal information using the web interface provided.

**<end of DG-BOOKING- 020>**

**<DG-BOOKING- 030>Inventory Availability Check**

The system shall verify in the background whether all the required equipment for the selected test is available in the inventory or not. If the equipment is not available, the system shall display this to the receptionist or patient immediately.

**<end of DG-BOOKING- 030>**

**<DG-BOOKING- 040>Payment Gateway Integration**

The system shall redirect the patient to the payment gateway user interface for online test booking. The payment gateway shall provide a secure interface for the patient to enter their payment details. The system shall receive the response from the payment gateway with https protocol.

**<end of DG-BOOKING- 040>**

**<DG-BOOKING- 050>Payment Terminal Integration**

For walk-in test bookings, the receptionist shall initiate payment, and the patient shall swipe their card at the payment terminal. The system shall communicate with the payment terminal using NDC protocol to verify the payment status.

**<end of DG-BOOKING- 050>**

**<DG-BOOKING- 060>Booking Details Encryption**

The system shall encrypt the booking details with AES 256 algorithm for security reasons. The booking details shall be securely stored in the database.

**<end of DG-BOOKING- 060>**

**<DG-BOOKING- 070>Database Management**

The system shall use MySQL server 8.0.32 for database management. The database shall store all the booking details securely.

Source: MYSQL

Version: 8.0.32

**<end of DG-BOOKING- 070>**

**<DG-BOOKING- 080>Notification API Integration**

The system shall use Mailosaur gateway for notification API integration. The notification API shall be hit with https protocol to send notifications to the patient about their test booking details.

Source: Mailosaur (<https://mailosaur.com/docs/api/messages/>)

**<end of DG-BOOKING- 080>**

**<DG-BOOKING- 090>Error Handling**

The system shall display an error message if the payment fails or if the required equipment is not available. The error message shall be displayed immediately to avoid any inconvenience to the patient.

**<end of DG-BOOKING- 090>**

**<DG-BOOKING- 100>Test Booking Confirmation**

The system shall send a notification to the patient about their test booking details, including the date and time of the test, the location of the laboratory, and any other relevant information. The notification shall be sent immediately after the booking is confirmed.

**<end of DG-BOOKING- 100>**

***1.3 Sample Collection***

**<DG-SAMPLE- 010>Authentication and Authorization**

The system shall provide login functionality for Lab Assistants to access the sample collection module. Only authorized users with Lab Assistants role shall be able to access the module and perform related actions.

**<end of DG-SAMPLE- 010>**

**<DG-SAMPLE- 020>Patient and Booking Details**

The system shall retrieve the patient and test booking details such as test name, date, time, and patient information such as name, age, gender, and contact details from the database. The test booking details shall be encrypted using AES 256 algorithm and decrypted before displaying to the Lab Assistant.

**<end of DG-SAMPLE- 020>**

**<DG-SAMPLE- 030>Inventory Management**

The system shall maintain an inventory of the required equipment for sample collection. The Lab Assistant shall be able to view the inventory status of the equipment and update it after taking it for sample collection.

**<end of DG-SAMPLE- 030>**

**<DG-SAMPLE- 040>Sample Collection**

The Lab Assistant shall be able to collect the sample from the patient based on the test booking details. The system shall have proper guidelines and instructions for the Lab Assistant to collect the sample accurately and safely. The Lab Assistant shall update the sample collection status in the system once the sample is collected.

**<end of DG-SAMPLE- 040>**

**<DG-SAMPLE- 050>Notification**

The system shall send a notification to the patient once the sample is collected successfully. The notification shall be sent via HTTPS protocol for security purposes.

**<end of DG-SAMPLE- 050>**

**<DG-SAMPLE- 060>QR Code Generation**

The system shall generate a unique QR code for each sample collected. The QR code shall include patient information such as patient id and test id. The QR code shall be generated using a QR code generator library.

**<end of DG-SAMPLE- 060>**

**<DG-SAMPLE- 070>Printing**

The QR code shall be printed on a label by a handheld QR code printer. The printer shall communicate with the system using IPP (Internet Printing Protocol) for printing the QR code accurately.

**<end of DG-SAMPLE- 070>**

***1.4 Performing Test***

**<DG-TESTING- 010>User Authentication**

The system shall allow lab technicians to log in to their machines with their unique credentials to access the application with a web interface.

**<end of DG-TESTING- 010>**

**<DG-TESTING- 020>Result Formats**

The system shall support various result formats such as text, image, video, pdf, and DICOM formats.

**<end of DG-TESTING- 020>**

**<DG-TESTING- 030>Web interface**

The software shall provide a web interface for lab technicians to access and interact with the system.

**<end of DG-TESTING- 030>**

**<DG-TESTING- 040>Report Generation**

The lab technician shall be able to generate reports by using patient details obtained from the QR code.

**<end of DG-TESTING- 040>**

**<DG-TESTING- 050>QR Code Scanning**

The system shall use a QR code scanner with a camera to scan the QR code and obtain the patient information.

**<end of DG-TESTING- 050>**

**<DG-TESTING- 060>Patient and Results Tagging**

The lab technician shall have a web interface to tag patient details with the generated results to generate a report.

**<end of DG-TESTING- 060>**

**<DG-TESTING- 070>Patient information retrieval**

The system should use a QR code scanner with camera to obtain patient information from the QR code generated during sample collection. This uses ZXing library.

**<end of DG-TESTING- 070>**

**<DG-TESTING- 080>Encryption**

The system shall encrypt the generated report data using AES 256 algorithm.

**<end of DG-TESTING- 080>**

**<DG-TESTING- 090>Notification API**

The system shall send notifications to users using a notification API gateway indicating that the test results and reports are ready.

**<end of DG-TESTING- 090>**

**<DG-TESTING- 100>User Role Access**

Only lab technicians shall have access to the lab workstation and perform test operations.

**<end of DG-TESTING- 100>**

***1.5 Reporting System***

**<DG-REPORTS- 010>User Roles and Access Control**

The reporting system shall provide three types of users: patients, doctors, and lab technicians. Each user role shall have its own login credentials and access level. The patients can view their reports only. The doctors can view their patients' reports and search the database for reports. Lab technicians can search, view and print reports.

**<end of DG-REPORTS- 010>**

**<DG-REPORTS- 020>Patient Authentication**

The system shall allow patients to log in using their unique credentials. The authentication process shall be secure and comply with industry best practices for protecting patient data.

**<end of DG-REPORTS- 020>**

**<DG-REPORTS- 030>Patient Report Viewing**

After logging in, patients shall be able to view a list of their reports on the web page. They shall be able to click on each report to view the report in their web browser. The report data shall be decrypted using the AES 256 algorithm, and the web user interface shall display images, videos, and DICOM files using the web-DICOM viewer.

**<end of DG-REPORTS- 030>**

**<DG-REPORTS- 040>Report Sharing via Email**

Patients shall be able to email their reports through the system. If a patient wants to email their report, the system shall use notification APIs to send the report to the patient's registered email. This functionality shall be secure and comply with industry best practices for protecting patient data.

**<end of DG-REPORTS- 040>**

**<DG-REPORTS- 050>Doctor Report Access**

The system shall allow doctors to search for their patients' reports using patient details. Once a report is found, the doctor shall be able to access and view the report by clicking on it. The report view shall support different file formats including image, video, pdf, and DICOM format.

**<end of DG-REPORTS- 050>**

**<DG-REPORTS- 060>DICOM Support**

For reports in DICOM format, the system shall use the web-DICOM viewer to display them. The viewer shall provide necessary functionalities for doctors to view and analyze the DICOM files in a user-friendly manner.

**<end of DG-REPORTS- 060>**

**<DG-REPORTS- 070>Lab Technician Access**

The system shall allow lab technicians to access the reporting system to search, view, and print reports. Lab technicians shall be able to log in using their unique credentials to access the system. Once logged in, they shall be able to search for reports using patient details.

**<end of DG-REPORTS- 070>**

**<DG-REPORTS- 080>Lab – Technician Report Viewing**

Lab technicians shall be able to view reports in different file formats including image, video, pdf, and DICOM format. The report view shall support necessary functionalities for lab technicians to view and analyze the reports. For DICOM files, the web-DICOM viewer shall be used.

**<end of DG-REPORTS- 080>**

**<DG-REPORTS- 090>Report Printing**

The system shall support printing of reports for lab technicians. Lab technicians shall be able to print reports using IPP printing as well as DICOM printing for X-rays.

**<end of DG-REPORTS- 090>**

***1.6 Inventory Manager***

**<DG-INVENTORY- 010>User Access**

Only the supervisor shall have access to the inventory manager. The supervisor shall be required to provide their unique credentials to log into the application using a web browser.

**<end of DG-INVENTORY- 010>**

**<DG-INVENTORY- 020>Inventory Item Addition**

The system shall have the capability to add new items to the inventory database. The items added to the inventory shall be saved in the database with relevant details such as name, description, quantity, and unit price.

**<end of DG-INVENTORY- 020>**

**<DG-INVENTORY- 030>Inventory Updation**

The system shall have the capability to update the inventory when the equipment was collected for sample collection or testing.

**<end of DG-INVENTORY- 030>**

**<DG-INVENTORY- 040>Threshold Setting**

The system shall allow the supervisor to set the thresholds for low stock levels for items in the inventory database. The supervisor shall be able to specify the minimum quantity of each item that should be maintained in the inventory.

**<end of DG-INVENTORY- 040>**

**<DG-INVENTORY- 050>Low Stock Monitoring**

The system shall monitor the stock levels of all items in the inventory database and compare them against the set thresholds.

**<end of DG-INVENTORY- 050>**

**<DG-INVENTORY- 060>Notification**

Whenever the stock level of any item falls below its threshold, the system shall notify the supervisor of the low stock level through a notification sent to their registered email or mobile number.

**<end of DG-INVENTORY- 060>**

**<DG-INVENTORY- 070>Inventory Reports**

The system shall allow the supervisor to generate reports on the inventory database. The reports shall provide detailed information on the current stock levels of all items in the inventory, the items that have breached their low stock threshold, and any other relevant details deemed necessary by the supervisor. The reports shall be available for viewing and/or printing in various formats such as PDF, CSV, or Excel.

**<end of DG-INVENTORY- 070>**

***2. Operations, Administration and Maintenance***

**<DG-OAM-010>Access Control Management**

The system shall allow the sysadmin to manage the access control matrix by defining actions for each role, specifying who can do what.

**<end of DG-OAM-010>**

**<DG-OAM-020>Data Export and Anonymization**

The system shall allow the sysadmin to export data by deidentifying and anonymizing it, ensuring the privacy and confidentiality of the data.

**<end of DG-OAM-020>**

**<DG-OAM-030>Encryption Key Management**

The system shall allow the sysadmin to rotate the encryption keys, ensuring the security and integrity of the data.

**<end of DG-OAM-030>**

**<DG-OAM-040>Application Management**

The sysadmin shall be able to upgrade and downgrade the application, ensuring the availability and performance of the system.

**<end of DG-OAM-040>**

**<DG-OAM-050>Account Management**

The sysadmin shall be able to manage the suspended accounts, ensuring the security and integrity of the data.

**<end of DG-OAM-050>**

**<DG-OAM-060>Password Policy Management**

The sysadmin shall be able to change the password policy based on the requirements, ensuring the security and confidentiality of the data.

**<end of DG-OAM-060>**

***3. Error Recovery***

**<DG-ERROR-010>Logging Mechanism**

The system shall have a logging mechanism to log all events in the application, ensuring traceability and accountability of the system.

**<end of DG-ERROR-010>**

**<DG-ERROR-020>Error Logging**

The system shall log error information to the logging mechanism, ensuring that errors are recorded and can be reviewed.

**<end of DG-ERROR-020>**

**<DG-ERROR-030>Error Detection and Notification**

The system shall detect errors when they are logged and send a notification to the sysadmin, ensuring timely resolution of errors.

**<end of DG-ERROR-030>**

**<DG-ERROR-040>Error Analysis**

The sysadmin shall be able to analyze errors from the logging mechanism, identifying the root cause of the error.

**<end of DG-ERROR-040>**

**<DG-ERROR-050>Root Cause Analysis**

The sysadmin shall be able to perform root cause analysis to identify the underlying cause of the error, ensuring effective resolution of errors.

**<end of DG-ERROR-050>**

**<DG-ERROR-060>Error Resolution**

The sysadmin shall determine the action to fix the error with the help of Subject Matter Experts (SMEs), ensuring effective resolution of errors.

**<end of DG-ERROR-060>**

**<DG-ERROR-070>System Recovery**

The sysadmin shall recover the system from the error by implementing the fix, ensuring that the system is fully functional and available for use.

**<end of DG-ERROR-070>**

***4. Security***

**<DG-SECURITY-010>Strong Password Policy**

The system shall enforce a strong password policy that requires users to create a secure password and regularly change it.

**<end of DG-SECURITY-010>**

**<DG-SECURITY-020>Authorization**

The system shall perform authorization for all the actions by verifying the user role with Access Control Matrix.

**<end of DG-SECURITY-020>**

**<DG-SECURITY-030>Data Encryption and Hashing**

The system shall encrypt and decrypt all the user data at rest with AES 256 algorithm and the password should be securely hashed with SHA256 algorithm.

**<end of DG-SECURITY-030>**

**<DG-SECURITY-040>Asymmetric Encryption**

The system shall possess asymmetric encryption with private and public keys for encrypting the data at motion.

**<end of DG-SECURITY-040>**

**<DG-SECURITY-050>Idle Timeout**

The system shall automatically logout the user if the idle time is more than 5 minutes.

**<end of DG-SECURITY-050>**

**<DG-SECURITY-060>Session Management**

The system shall delete the session token on the client side after user logging out.

**<end of DG-SECURITY-060>**

**<DG-SECURITY-070>Data Packet Validation Requirement**

The system shall be able to validate the checksum of the incoming data packets.

**<end of DG-SECURITY-070>**

**<DG-SECURITY-080>Request Denial Requirement**

The system shall deny the request if the checksum in the header and checksum of data is not matching and this should be logged for further analysis.

**<end of DG-SECURITY-080>**

**<DG-SECURITY-090>Account Suspension**

The system shall suspend the user account for malicious activity.

**<end of DG-SECURITY-090>**

***5. Performance***

**<DG-PERFORMANCE-010> Monitoring System Resources and KPI Metrics**

The system shall be capable of monitoring the system resources, such as CPU usage, memory usage, and disk space, as well as other Key Performance Indicators (KPIs) such as response time and throughput.

**<end of DG-PERFORMANCE-010>**

**<DG-PERFORMANCE-020> Setting Alert Thresholds**

The sysadmin shall be able to set the thresholds for alerting to the monitoring system, specifying the acceptable range of values for each monitored metric.

**<end of DG-PERFORMANCE-020>**

**<DG-PERFORMANCE-030> Alert Notifications**

The system shall notify the sysadmin via email, SMS, or other notification system, if any threshold is breached, providing relevant details such as the name of the metric, the value, and the time of the breach.

**<end of DG-PERFORMANCE-030>**

**<DG-PERFORMANCE-040> Database Concurrency**

The sysadmin shall be able to increase the concurrency in the database connections for high performance, by configuring the database connection pool size or other relevant parameters.

**<end of DG-PERFORMANCE-040>**

**<DG-PERFORMANCE-050> Load Balancing and Autoscaling**

The sysadmin shall configure a load balancer and auto scale the servers for handling more traffic, ensuring high availability and scalability of the system.

**<end of DG-PERFORMANCE-050>**

**<DG-PERFORMANCE-060> Application Updates**

The sysadmin shall update the application to the newer versions for optimized performance, applying patches, bug fixes, and feature enhancements as needed.

**<end of DG-PERFORMANCE-060>**

**<DG-PERFORMANCE-070> Database Tuning**

The sysadmin shall tune the database by indexing the database, implementing caching, and increasing the buffer size, to improve query performance and reduce I/O operations.

**<end of DG-PERFORMANCE-070>**

**<DG-PERFORMANCE-080> Hardware Upgrades**

The sysadmin shall optimize the application performance by upgrading to new hardware, such as faster CPUs, more memory, or solid-state drives, to increase processing speed and reduce latency.  
**<end of DG-PERFORMANCE-080>**

***6. Availability and Reliability***

**<DG-AVAILABILITY-RELIABILITY-010> Monitoring SLA Metrics**

The system shall continuously monitor the key SLA metrics of the system which includes response time, availability, and throughput. The system shall capture these metrics in real-time and store them for later analysis.

**<end of DG-AVAILABILITY-RELIABILITY-010>**

**<DG-AVAILABILITY-RELIABILITY-020> Threshold Configuration**

The sysadmin shall have the ability to set thresholds for each SLA metric to trigger an alert in case of breach.

**<end of DG-AVAILABILITY-RELIABILITY-020>**

**<DG-AVAILABILITY-RELIABILITY-030> Notification Alert**

The system shall send a notification via SMS or email alert to the sysadmin if any of the SLA metrics are breached. This notification shall include information about the metric that has been breached, the severity level of the breach, and the time when the breach occurred.

**<end of DG-AVAILABILITY-RELIABILITY-030>**

**<DG-AVAILABILITY-RELIABILITY-040> Backup Provisioning**

The sysadmin shall take backups of the system by creating snapshots of the application server and database. These snapshots shall capture the entire state of the application server and database at a given point in time, including all data, configurations, and settings.

**<end of DG-AVAILABILITY-RELIABILITY-040>**

**<DG-AVAILABILITY-RELIABILITY-050> Storage Management**

The sysadmin shall store the snapshots in a highly available storage solution. This storage solution shall provide high durability, availability, and scalability to ensure that the backups are accessible at all times, even in case of hardware or network failures.

**<end of DG-AVAILABILITY-RELIABILITY-050>**

**<DG-AVAILABILITY-RELIABILITY-060> Synchronization Configuration**

The sysadmin shall configure synchronization between the main application server, database, and cloned application server and database, for disaster recovery purposes. This synchronization shall ensure that the data and configurations of the main and cloned environments are kept in sync, to minimize the downtime in case of a disaster.

**<end of DG-AVAILABILITY-RELIABILITY-060>**

**<DG-AVAILABILITY-RELIABILITY-070> Recovery Provisioning**

The sysadmin shall be able to recover the system in case of failure by provisioning the application server and database and restoring it from the latest snapshot from the backup manager.

**<end of DG-AVAILABILITY-RELIABILITY-070>**

**<DG-AVAILABILITY-RELIABILITY-080> Disaster Recovery Redirection**

The sysadmin shall redirect all traffic to the DR (disaster recovery) environment in case of a disaster, and if the application cannot be recovered from the current live production environment.

**<end of DG-AVAILABILITY-RELIABILITY-080>**