School of Computer Science & Software Engineering

Bachelor of Computer Science (Cybersecurity)

CSCI321- Project

Project Requirement Specification

[8th Nov 2025]

Group: FYP-25-S4-17

Chen Yongfeng	8575575	ychen212@mymail.sim.edu.sg
Gurkeeratjit Singh Togar	8334572	togar002@mymail.sim.edu.sg
Karen Wirjo	8576129	kwirjo001@mymail.sim.edu.sg
Lin Jia Cheng, Shawn	8576610	jcslin001@mymail.sim.edu.sg
Wgen Tan	8769266	wtan049@mymail.sim.edu.sg

Supervisor: Yeo Sze Wee Aaron

Assessor: Tian Sion Hui

1 Document Control

1.1 Distribution List

Name	Title/Role	Location of where the document is stored
Tian Sion Hui	Assessor	NA
Yeo Sze Wee Aaron	Project Supervisor	NA
Karen Wirjo	Project Manager	NA
Wgen Tan	Document Lead	NA
Gurkeeratjit Singh Togar	Design Engineer	NA
Lin Jia Cheng, Shawn	Programmer Lead	NA
Chen Yongfeng	QA Team Lead	NA

1.2 Record of Revision

Revision Date	Description	Section Affected	Changes Made by	Version after Revision
Oct 15	Assign Roles, identify users	Project background and project plan	Everyone	1.0
Oct 16	Added executive summary and glossary	Executive Summary and Glossary	Everyone	1.1
Oct 17	Added project background	Project Background	Everyone	1.2
Oct 18	Added market research	Market Research	Wgen	1.3
Oct 19	Added platform functionality, proposed product feature and capabilities	Platform Functionality, Proposed product feature and capabilities	Karen	1.4
Oct 20	Added work breakdown structure, product diagrams Updated market research	WBS, product diagrams, market research	Karen, Wgen, Keerat	1.5
Oct 21	Added project vision, goals	Project vision,	Karen	1.6

	and risk analysis	goals, risk analysis		
Oct 22	Added software development methodology, project deliverables project plan and proposed project organisation	Software Development methodology, project deliverables, project plan, proposed project organisation	Karen	1.7
Oct 27	Added functional requirement, non functional requirement, use case diagrams, user stories and use case description	Functional Requirement, Use-case Diagrams, User Stories, Use-Case Descriptions	Chen YongFeng, Shawn	1.8
Oct 28	Added more user stories Updated work breakdown structure and product diagram	Applicable User Stories, WBS, Product Diagram	Karen, Wgen	1.9
Oct 29	Updated use case diagrams Added use case description, performance, security and usability	Use case Diagrams, Use-case description	Chen YongFeng, Shawn	2.0
Oct 30	Added reliability, scalability, maintainability and availability Updated glossary	Reliability, Scalability, Maintainability, and Availability, Glossary	Chen YongFeng, Shawn, Keerat	2.1
Oct 31	Added more user stories	Applicable User Stories	Everyone	2.2
Nov 1	Updated work breakdown structure and product diagrams Updated Executive Summary, and Glossary	WBS, Product Diagrams	Wgen, Karen, Keerat	2.3
Nov 2	Added use case description Updated use case diagrams	Product Requirements Specification	Shawn, Chen YongFeng	2.4
Nov 3	Added user interface requirements, future enhancement	Product Requirements Specification, Future Enhancement	Karen, Shawn	2.5

Nov 4	Updated use case description, diagrams and user stories Updated glossary, executive summary, platform functionality	Product Requirements, Specification Glossary, Project Background	Shawn, Chen YongFeng, Keerat	2.6
Nov 5	Updated work breakdown structure and product diagrams Updated future patient, hospital, system administrator, system security, health researcher user stories integration	Project Proposal, Future Enhancement	Everyone	2.7
Nov 6	Finalised user stories and all diagrams Updated glossary Added references	All	Everyone	2.8
Nov 7	Fixed Formatting, Wording, Table Structure	All	Everyone	2.9
Nov 8	Finalised document	All	Everyone	3.0

2 Table of Contents

3 Executive Summary

This document provides the Project Requirements Specification for a web-based healthcare application utilizing Private Set Intersection technology. The document clearly defines the system's objectives and requirements as well as ensures that all stakeholders share a common understanding of what the system will achieve and how it will operate.

In the healthcare sector, sensitive data such as genetic information and patient health records must be handled with strict privacy and compliance to data protection regulations. The proposed system aims to enable hospitals, patients, and research institutions to identify common genes or health data patterns without revealing their complete datasets. By integrating PSI techniques into a web application, the project promotes secure and privacy preserving data collaboration for research and diagnosis, helping to uncover medical insights without compromising individual privacy.

The objective of this project is to develop a fully functional and deployable web application that allows users to perform secure data comparisons and risk assessments based on genetic information. The system will support multiple user roles to upload, analyze, and interpret results through an intuitive interface while maintaining data confidentiality. To achieve this, the document outlines the functional requirements and non-functional requirements and any other requirements relevant to healthcare applications.

This document covers 6 sections, the introduction, glossary, overview, requirements definition, Functional Requirements, non functional requirements, other requirements and appendix

This specification document provides a comprehensive foundation for guiding the design, development, and evaluation of the PSI healthcare system.

4 Glossary

AES (Advanced Encryption Standard): A standard method for scrambling (encrypting) digital data using a secret key so only someone with the key can unscramble.

Anonymized Data: Data that has had all personal identifying information removed so that individuals cannot be recognized.

Authentication: Confirming that someone is who they claim to be (for example, by checking a username and password).

Authorization: Determining which actions or resources a verified (authenticated) user is allowed to access.

Cryptographic Key Management: The process of creating, sharing, storing, and updating the secret keys used for encryption, to keep them safe and ensure data stays secure.

Data at Rest: Data that is stored on a device or disk (not currently being sent over a network) and must be protected.

Data in Transit: Data that is moving over a network (such as the Internet) and must be protected while it travels.

Diffie-Hellman: A well-known cryptographic method that lets two parties agree on a shared secret and compare data securely without revealing their private inputs.

Diffie-Hellman–based PSI: A specific Private Set Intersection method that uses the Diffie-Hellman cryptographic technique to compare datasets privately (so neither party learns the other's data, only the common elements).

Disease-Gene Database: A list of genes maintained by a hospital that are known to be linked to specific diseases.

DNA Sequencing: The process of determining the order of the building blocks (bases) in DNA; the raw result is the genetic data that users upload for analysis.

DNA / Genetic Marker: A specific gene or DNA pattern that is known to be associated with a particular trait or disease.

Direct-to-Consumer (DTC) Genetic Test: An at-home genetic test kit that consumers buy themselves (for example, for ancestry or health); the raw genetic data from such tests can be uploaded into the system.

End-to-End Encryption: A security approach where data is encrypted by the sender and only decrypted by the intended recipient, ensuring it remains unreadable while in transit between systems.

Encryption: The process of converting readable data into a coded form so that only someone with the right key can turn it back into readable form.

Frontend / Backend: In a web application, the frontend is the part users interact with in their browser (the user interface), and the backend is the server-side system that stores data and runs the logic.

General Data Protection Regulation (GDPR): A European Union law that sets rules for how personal data must be collected, used, and protected.

Health Insurance Portability and Accountability Act (HIPAA): A U.S. law that establishes federal rules to keep people's private health information confidential and secure.

Multi-Factor Authentication (MFA): A security practice requiring two or more methods of verifying a user's identity when logging in (for example, a password plus a code sent to the user's phone).

Personal Data Protection Act (PDPA): Singapore's law that regulates how personal information can be collected, used, and shared to protect individual privacy.

Privacy-Preserving Computation: Techniques (such as Private Set Intersection) that allow two parties to jointly compute a useful result without revealing their underlying private data to each other.

Private Set Intersection (PSI): A cryptographic method that lets two parties find out which items they have in common (their set intersection) without revealing anything else about their private datasets.

Rate Limiting: A control mechanism that restricts how many requests or operations a user can perform in a given time period, to prevent abuse or overload.

Role-Based Access Control (RBAC): An access control method where users are given permissions based on their role (for example, patient, hospital administrator, or security officer).

Real-Time Processing: Computing results immediately as new data arrives, so users get timely feedback or analysis without long delays.

Scalable Architecture: Designing a system so that more computing resources (like servers) can be added easily, allowing the system to handle many more users or data without a major redesign.

Security Testing (Penetration Testing): Tests (often called pen tests) where security experts try to attack or break into the system in a controlled way, to find and fix vulnerabilities before malicious attackers do.

Session Management / Session Timeout: How a web application tracks user login sessions and automatically logs users out after a period of inactivity, as a security precaution.

Transport Layer Security (TLS): A standard internet protocol (used, for example, in HTTPS) that encrypts data sent over a network to protect it from eavesdroppers.

Verification / Audit Logs: Records kept by the system that track who did what and when; these logs are used to check compliance with rules and to troubleshoot problems.

5 Project Background

5.1 Project Objective

Our main objective is to develop an application that would allow patients to securely share their health information with hospitals without compromising their data or their identity. The application uses the Diffie-Hellman based Private Set Intersection (PSI) protocol to ensure that neither the patient nor the hospital have access to each other's sensitive information, while ensuring privacy and accurate calculations.

5.2 Learning Objective

The group will learn how to communicate effectively with the clients to design and program an application that meets the client's needs. In addition, the group will learn to apply problem solving skills, as well as, consolidate knowledge they have previously acquired.

5.3 Target Audience

Patients who wish to privately determine their risk of having a particular disease without having to reveal their genetic information and Organisations that wish to provide risk assessment services without disclosing their discoveries.

5.4 Problem Description

Privacy Issues
Due to the sensitive nature of medical data, there are often concerns about their security, privacy, ethicality and legality when stored in large databases. Data leakage from these databases can have serious implications on the patients and/or their caregiver's lives. Including, but not limited to loss of jobs, poor social networking and lack of employment.

5.5 Proposed Solutions

Diffie-Hellman based Private Set Intersection (PSI)
An app that calculates the risk of a disease by combining the cryptographic technique of Private Set Intersection (PSI) with the Diffie-Hellman (DH) key exchange protocol. The DH based PSI ensures that neither the patient, the hospital, nor any third party, has access to any sensitive information during risk assessment calculation.

PDPA

The Personal Data Protection Act (PDPA) dictates the criteria for the collection, usage and disclosure of personal data in Singapore. This aims to prevent the misuse of personal data and to establish trust between individuals and organisations. Breach of the PDPA may result in a heavy financial penalty of up to 10% of the organisation's turnover.

To comply with the PDPA, our app will implement the following.

1. Users will be informed, through the privacy policy, on how data is collected, stored and used. Explicit consent is required before the collection, usage and disclosure of any personal data.
2. Users will have full access to their personal data and are able to review and edit their data upon request.
3. Steps are taken to ensure that all personal data are well protected and secure. Appropriate administrative and security personnel will be appointed to protect data from unauthorised access, use, disclosure, alteration or destruction.
4. All data collected, with the exception of those regarding business or legal purposes, will be securely deleted when it is no longer needed.

5.6 Market Research

The majority of healthcare applications on the market primarily focus on helping users manage their medical information (i.e appointments, bill payments, medical records, medications and other administrative tasks). Whilst these are useful features for a healthcare application, they do not address the more personalised and preventive healthcare needs that patients may desire.

To better understand the current market and demand for our product, we have included companies that provide risk assessment services, applications with similar features and popular healthcare applications in our research.

5.6.1 NUHS (National University Health System)

A mobile healthcare app developed by the National University Health System (NUHS) and Synapxe Pte. Ltd. (formerly known as Integrated Health Information Systems Pte Ltd) that enables patients to manage and take charge of their health. It allows their users access to a range of healthcare services across 14 NUHS institutions.

NUHS		
No.	**Features**	**Description**
Appointments		
1	Appointment registration	Users can register and check their medical appointments through the app
2	Mobile registration	Users can register and check their queue status when going for appointments
3	Reschedule appointment	Users can reschedule their appointments through the app
4	Cancel appointment	Users can cancel their appointments through the app
5	Teleconsultation	Users can register for an online consult on Zoom 30 minutes before their appointment
Bill Payments		
6	Make payment	Users can view and pay their bills through the app
7	Download invoice	Users can download their invoice for claims' submission
8	Payment status and history	Users can track their payment status and history of up to 12 months
9	Pay on behalf of others	Users can pay on behalf of their family and friends by using the bill reference number
Medication		
10	View medications	Users can view their current medication list, prescribed dosage, and their instructions
11	Request for medication refills or top-ups	Users can order their prescribed medication top-ups and refills through the app and choose either self-collection or delivery
Medical Records		

12	Access medical reports	Users can request and download their medical reports directly from the app
13	Access Medical Certificates (MC)	Users can view and download a digital copy of their MCs directly from the app
14	Access letters	Users can view and download a digital copy of their letters directly from the app
15	After visit summary	Users can view and download a digital copy of their after visit summary directly from the app
Caregiver Access		
16	Add caregiver	Users can add the details of their caregivers to allow them access to the users health records and transactions
17	Add dependent	Users can add the details of their dependent to access the dependent's health records and transactions
Emergency Visit		
18	Check wait time	Users can check the wait time of the Emergency Department before their arrival
19	Health declaration form	Users can complete the health declaration form before their emergency visit through the app

5.6.2 HealthHub

HealthHub is the national healthcare app in Singapore that enables Singaporeans to manage theirs and their loved ones' health. It allows their users access to their health records and services of public healthcare institutions.

HealthHub SG		
No.	**Features**	**Description**
Appointments		
1	View appointments	Users can view their appointment details
2	Make appointments	Users can make appointments at healthcare institutions through the app
3	Reschedule appointment	Users can reschedule their appointments through the app
4	Cancel appointment	Users can cancel their appointments through the app
5	Pre-register appointments	Users can get a queue number and check its status before their appointment
Payment		
6	Make Payment	Users can pay for their bills throught the app
7	Payment details	Users can view their payment details after their appointment
8	Download receipt	Users can download their receipts after they make payment
9	Payment history	Users can view their payment status and history through the app
Prescriptions		
10	View Prescription	Users can view their past prescribed medications on the app
11	Request to refill/renew prescriptions	Users can request to refill or renew their prescription through the app
Health Records		
12	Access health records	Users can get an overview of their health records (general and selected lab tests)
Manage Loved ones' health		

13	Add caregiver	Users can add the details of their caregivers to allow them access to the users health records and transactions
14	Add dependent	Users can add the details of their dependent to access the dependent's health records and transactions

5.6.3 Genomapp

Genomapp is an app that provides DNA analysis service at a cost. Users are able to upload the raw DNA data they obtained from Direct-to-Consumer (DTC) genetic tests and gain an insight into their genetic code.

Genomapp		
No.	**Features**	**Description**
1	Upload file	Users can share the genetic file (raw data) they received from Direct-to-Consumer (DTC) genetic testing services
2	Report categories	Users can choose the type of report they wish to receive (with traits, observable signs and blood groups being free)
3	Privacy	Users can be certain that their DNA data remains securely in their device and not uploaded to the server or shared with another party
4	Demo mode	User can try out a sample version of the app before uploading their data or purchasing any reports
5	Database	Users can search among the wide variety of conditions, genes and genetic markers available on the app
6	Export PDF	Users are able to export the reports to PDF for printing or storage

5.6.4 Genexsure

Genexsure is a Tennessee based healthcare company that provides genetic testing and counselling.They offer their services directly to patients as well as through partnered hospitals and clinics.

Genexsure		
No.	**Features**	**Description**
1	Family member genetic testing	Users can get tested for diseases they suspect are inherited
Genetic Test Result Consultation		
2	Expert evaluation of family history	Users can get a genetic expert evaluation or theirs and their family's medical history
3	Personalised genetics risk report	Users can receive a personalised report detailing their risk of certain diseases based on their family's genes or history
4	Testing recommendations	Users can get recommendations from a genetic expert on tests they or their family could take
Genetic Consultation and Testing		
5	Expert evaluation of medical history	Users can get a genetic expert to evaluate their risk of inherited diseases based off theirs and their family's medical history
6	Evaluation of prior test reports	Users can have their genetic or ancestry test results analysed by genetic experts
7	Results review and additional testing	Users can get a genetic report explaining their genetic risks that include recommendations for medical grade testing

5.6.5 Invitae

Invitae is a collaboration between Labcorp and Invitae, two leaders in genetics, to provide genetic testing for a variety of diseases. Their services are marketed towards Individuals & Patients, Providers, Health Systems & Organisations and Biopharma & Investigators.

Invitae		
No.	**Features**	**Description**
1	Test catalogue and menu	Users can access a variety of genetic tests from both Labcorp and Invitae
2	Test ordering	Users can easily order tests for diseases to take at home
3	Genetic counselling	Users can receive guidance from genetic counsellors on the testing options, risks and results
4	Virtual consult	Users can consult a telehealth clinician on what test they should take
5	Fast turnaround testing	Users can expect to receive their test results within 3 weeks of testing
6	Comprehensible clinical report	Users can expect to receive a clear and transparent clinical report, detailing the performance characteristics for each condition or gene

Companies like Genexsure and Invitae provide their users genetic testing risk assessments service which gives them an insight into their genetic makeup. However, these services require users to upload their health data into external servers which brings up issues regarding privacy and security.

Genomapp, on the other hand, allows users to conduct risk assessments on their genetic data while ensuring that the data is purely stored in the user's device and not uploaded to an external server. However, Genomapp does not promise secure computation between the users and the institute, nor do they allow inputs from medical institutes into its disease database.

Applications like NUHS and HealthHub primarily focus on helping users manage their medical information, there are certain features, such as appointment management and caregiver access that may be good additions to our product further down the line.

Our proposed product would be a combination of the above. It provides multi-disease genetic risk assessment while ensuring privacy and security. Unlike Genexsure and Invitae, genetic data would be stored in the user's device, eliminating the risk of potential data breaches. And unlike Genomapp, by allowing secure collaborations with medical institutes, we can provide more accurate risk assessments to our users. In the future, we plan to include features such as caregiver access and appointment management like NUHS and HealthHub, which allow for a more centralised and user-friendly experience.

5.7 Platform Functionality

Features	NUHS	HealthHub	Genomapp	Genexsure	Invitae	Proposed Features
Account Management	✔	✔	✔	✔	✔	✔
Appointment Management	✔	✔		✔	✔	
Bill Payment	✔	✔		✔	✔	
Payment History	✔	✔		✔	✔	

Medication Management	✔	✔				
Disease Gene Database				✔	✔	✔
Genetic Data Management			✔			✔
Privacy Preserving Computation						✔
Local Data (not uploaded to server)			✔			✔
Risk Assessment			✔	✔	✔	✔
Multi-Disease Analysis			✔	✔	✔	✔
Risk Result Explanation			✔	✔	✔	✔
Export Reports	✔	✔	✔	✔	✔	✔
Assessment History	✔	✔	✔	✔	✔	✔
Family Member Access	✔	✔		✔	✔	
Genetic Testing				✔	✔	

Genetic Counselling				✔	✔	
Teleconsultation	✔	✔	✔	✔	✔	

6 Project Proposal

6.1 Proposed Product Features and Capabilities

The Private Set Intersection (PSI) for Healthcare Application is a web-based platform designed to enable secure and privacy-preserving disease risk assessments based on genetic data. The system leverages cryptographic PSI protocols to allow patients to identify their disease risk without revealing their complete genetic profile to hospitals, and similarly, hospitals can provide risk assessments without exposing their proprietary disease-gene databases.

No.	Feature	Implementation	Description
Patients			
1	Secure Account Management	Yes	Registration, login, logout, and password recovery with strong authentication mechanisms. Includes viewing and updating account details, and permanent account deletion.
2	Genetic Data Upload	Yes	Secure upload of gene sets for PSI-based risk assessment with support for common genetic data formats.
3	Disease Risk Assessment	Yes	Receive percentage-based risk calculations for specific diseases using PSI protocols.
4	Risk Explanation Interface	Yes	Clear presentation of risk assessment results with explanatory text about what percentages mean and recommended next steps.
5	Disease Search	Yes	Search functionality to find specific diseases or categories for targeted risk assessment.
6	Multi-Disease Analysis	Yes	Select and analyze risk for multiple diseases in a single

			session without repeating upload process.
7	Data Control	Yes	Delete uploaded genetic data after receiving results to maintain control over personal information.
8	Assessment History	Yes	View history of past genetic assessments and actions taken, tracking risk profile changes over time.
9	Report Export	Yes	Export risk assessment results as images or PDF reports for saving and sharing.
10	Appointment Booking	Yes	Book appointments with relevant specialists immediately after receiving genetic risk results.
11	Appointment Management	Yes	View, reschedule, and cancel appointments. View details of upcoming and past appointments.
12	Appointment Scheduling	Yes	View available appointment slots with specialists to choose convenient times.
13	Notification System	Yes	Receive notifications and reminders about upcoming appointments and important updates.
Hospitals/Healthcare Providers			
14	Hospital Authentication	Yes	Secure login, logout, and password reset functionality for hospital administrators.
15	Organization Registration	Yes	Register hospital organization on the platform to provide disease risk assessment services.

16	Hospital Account Management	Yes	View and update organization account details, contact information, and administrator credentials. Ability to deactivate hospital accounts when needed.
17	Disease Gene Database Management	Yes	Comprehensive CRUD operations for disease gene databases including viewing, adding, editing, and organizing gene entries.
18	Gene Categorization	Yes	Create, view, update, and delete disease categories. Organize genes by disease type (cardiovascular, oncological, neurological, etc.).
19	Gene Search	Yes	Search functionality to quickly locate specific genes in the database for updates or verification.
20	Category Search	Yes	Search for specific disease categories to efficiently manage large databases.
21	PSI-Based Risk Calculation	Yes	Securely provide disease risk calculations to patients using PSI protocols without accessing private genetic data.
22	Database Verification	Yes	Verify that the system is using disease gene databases correctly to ensure accurate patient results.
23	Database Updates	Yes	Add newly discovered disease-associated genes and edit existing entries (risk coefficients, metadata) based on latest research.

24	Batch Processing	Yes	Efficiently process multiple patient requests to serve many patients without long wait times.
25	Specialist Scheduling	Yes	Manage specialist availability and appointment slots for patient bookings.
26	Appointment Viewing	Yes	View all scheduled appointments with patients to manage specialist schedules and prepare for consultations.
Healthcare Researchers			
27	Data Filtering	Yes	Filter PSI results based on specific criteria (age, location, disease type) to focus research on targeted populations.
28	Data Visualization	Yes	Visualize aggregated PSI results in dashboards to analyze patterns and trends without accessing raw patient data.
29	Data Export	Yes	Export anonymized PSI results into standard formats (CSV, JSON) for integration with existing research tools.
System Administrators			
30	Hospital Approval System	Yes	Approve or reject hospital registration requests to ensure only legitimate healthcare providers access the system.
31	User Management	Yes	Comprehensive user account management including viewing all users, resetting passwords, updating account information,

			suspending/deactivating accounts, and creating admin/security accounts.
32	Audit Logging	Yes	Maintain audit logs of all calculations and system actions for compliance and accuracy verification.
33	System Monitoring	Yes	Monitor system performance, data usage, and health to ensure smooth operation without downtime.
34	Alert System	Yes	Receive instant alerts when the PSI system goes down for quick restoration of services.
35	Data Backup System	Yes	Perform regular backups of system data for recovery in case of data loss or corruption.
36	Usage Analytics	Yes	Generate monthly usage and performance reports to track system health and prepare for audits.
37	Appointment Analytics	Yes	View analytics on appointment bookings, cancellations, and no-shows to identify usage patterns and resolve scheduling conflicts.
38	Rate Limiting	Yes	Set rate limits on PSI computations per user per day to prevent system abuse and ensure fair resource allocation.
System Security Users			
39	Cryptographic Key Management	Yes	Manage and rotate cryptographic keys used in PSI to maintain secure data

			exchanges between healthcare providers.
40	Encryption Enforcement	Yes	Enforce encryption of all data at rest and in transit to protect sensitive healthcare data from unauthorized access.
41	Access Control	Yes	Enforce role-based access control (RBAC) so only authorized staff can access or configure sensitive components.
42	Multi-Factor Authentication (MFA)	Yes	Implement MFA for hospital administrator accounts to protect disease gene databases from unauthorized access.
43	Anomaly Detection	Yes	Monitor PSI logs for anomalies and implement secure logging and audit trails for all operations.
44	Security Alert System	Yes	Receive automated alerts for suspicious PSI activities to respond quickly to potential security breaches.
45	Security Policy Management	Yes	Periodically review and update system security policies to comply with evolving privacy laws and standards.
46	Compliance Reporting	Yes	Generate compliance and audit reports of PSI transactions to demonstrate adherence to privacy regulations.
47	Security Testing	Yes	Conduct regular penetration tests to identify and fix vulnerabilities before attackers exploit them.

48	Incident Response	Yes	Automatically isolate and contain compromised accounts or systems to minimize damage and prevent breach spread.
Technical Capabilities			
49	Diffie-Hellman Based PSI Protocol	Yes	Implementation of cryptographic PSI protocol for secure genetic data comparison without revealing complete profiles.
50	End-to-End Encryption	Yes	All data transmissions are encrypted from patient device to hospital systems and vice versa.
51	Scalable Architecture	Yes	Cloud-based infrastructure supporting horizontal scaling to accommodate growing user base and data volume.
52	Real-Time Processing	Yes	Optimized PSI computations providing risk assessment results within acceptable timeframes.
53	Compliance Framework	Yes	Built-in compliance with HIPAA, GDPR, and PDPA regulations for healthcare data protection.

6.2 Product Diagram

The product we are developing is a web-based healthcare application that implements Private Set Intersection (PSI) technology for secure genetic disease risk assessment. The purpose of this application is to enable patients to determine their risk of developing specific diseases based on their genetic information, while ensuring complete privacy for both the patient's genetic data and the hospital's disease-gene databases.

The system facilitates secure collaboration between patients, hospitals, research institutions, and system administrators to enable privacy-preserving genetic analysis and disease risk assessment. By utilizing the Diffie-Hellman based PSI protocol, the application allows two parties (patient and hospital) to compute the intersection of their genetic datasets without revealing the complete contents of either dataset to the other party.

Patients are required to register using their personal information including email address and password. After account creation, patients can securely upload their gene set obtained from DNA sequencing (e.g., $X = \{x_1, x_2, ..., x\square\}$). The application performs PSI computation with the selected hospital's disease-gene database to calculate the patient's disease risk as a percentage ($c|X \cap Y|/n$ %), where matching genes indicate increased disease risk. Patients can view their risk assessment results, export them as reports, book specialist appointments, and manage their genetic data with full control over deletion and privacy.

Hospitals/Healthcare Providers register their organizations to provide disease risk assessment services. They maintain secure disease-gene databases containing genes ($Y = \{y_1, y_2, ..., y\square\}$) that are associated with specific diseases. Hospitals can manage their gene databases by adding newly discovered disease-associated genes, categorizing genes by disease type (cardiovascular, oncological, neurological, etc.), and updating risk coefficients based on latest research. The PSI protocol ensures that hospitals can provide accurate risk calculations to patients without ever accessing the patients' complete genetic profiles.

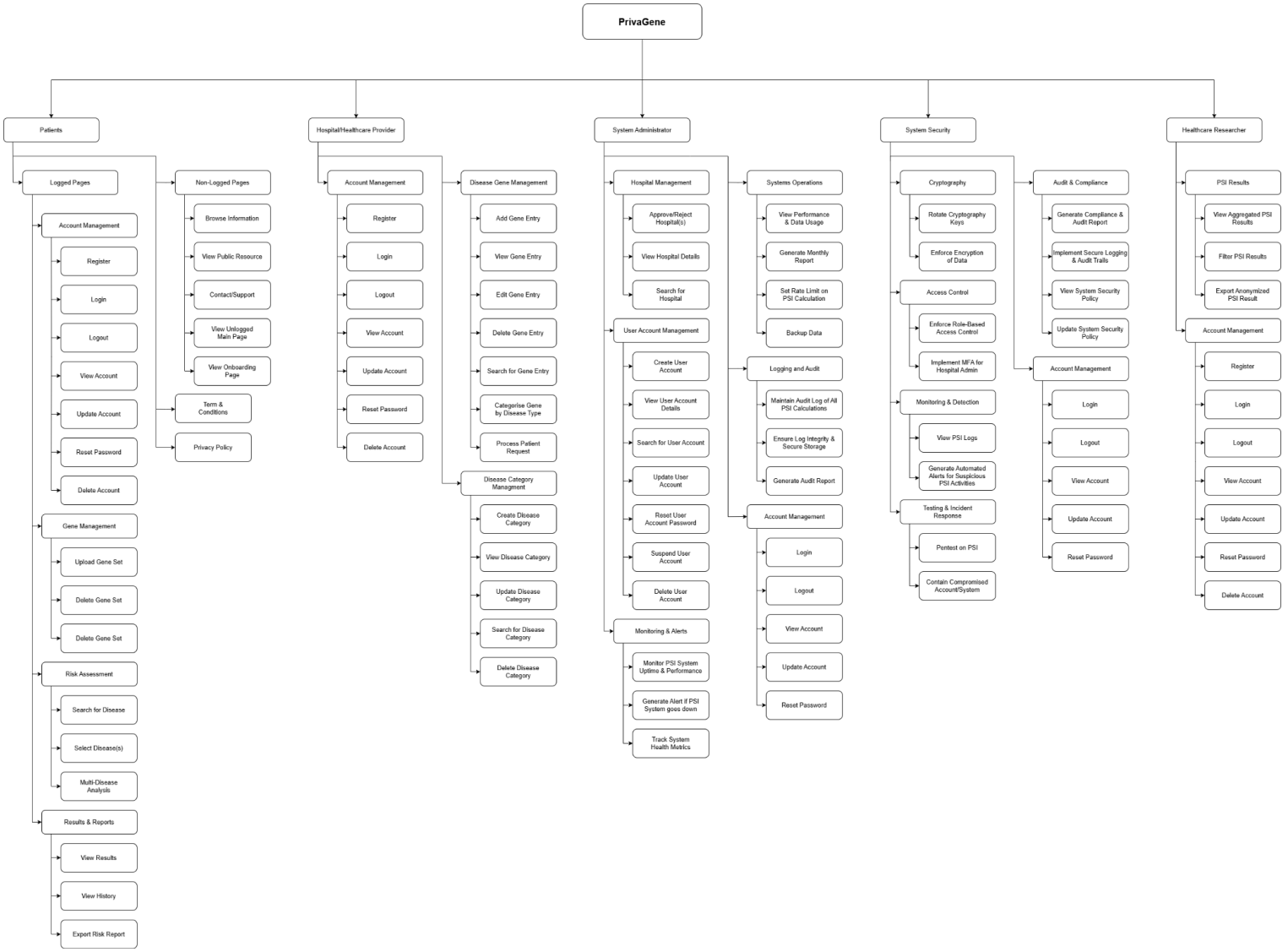
System Administrators oversee the entire platform by approving hospital registrations, managing user accounts, monitoring system performance, maintaining audit logs of all PSI computations, and ensuring compliance with healthcare data privacy regulations. They perform regular system backups, implement rate limiting to prevent abuse, and generate monthly usage reports.

System Security Users are responsible for managing cryptographic keys used in PSI protocols, enforcing encryption of all data at rest and in transit, implementing role-based access control, monitoring for security anomalies, conducting penetration tests, and ensuring the platform adheres to evolving privacy laws and healthcare data protection standards.

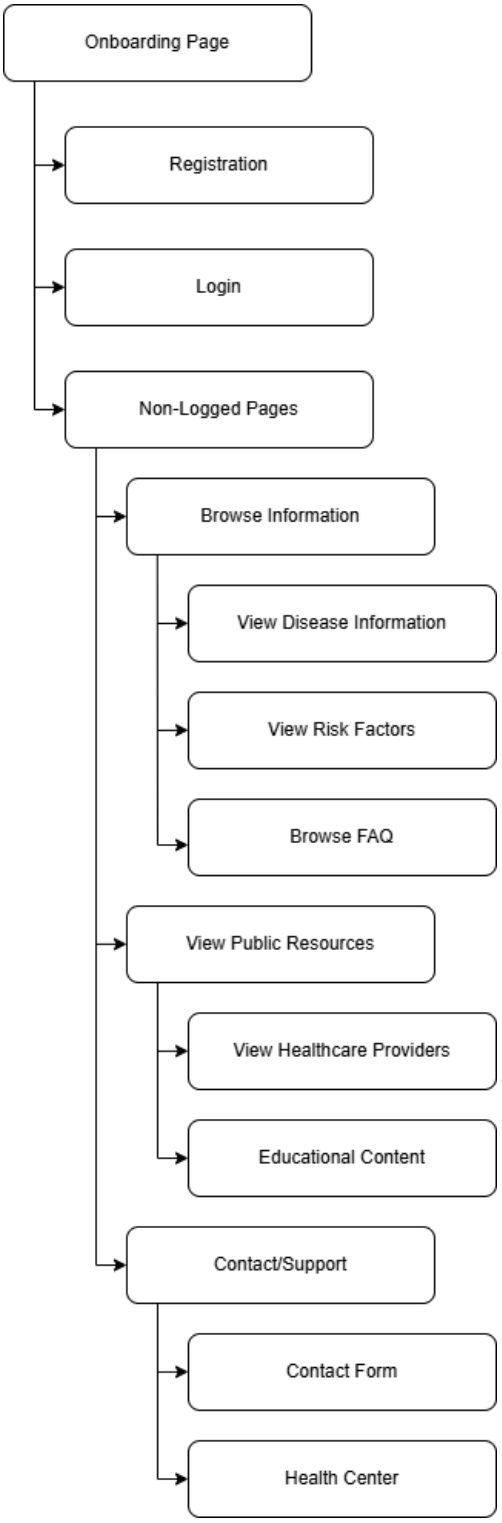
Health Research Agencies can utilize the platform to conduct collaborative research by running PSI protocols with partner hospitals to identify overlapping gene sets for joint research studies without exposing individual patient data. They can match hospital genetic databases with national health databases to identify disease-gene associations while preserving patient privacy, and contribute to global health studies while maintaining compliance with local privacy regulations.

The application supports multiple user roles with distinct permissions and features to ensure secure, privacy-preserving genetic data analysis while maintaining data confidentiality and regulatory compliance throughout the entire process.

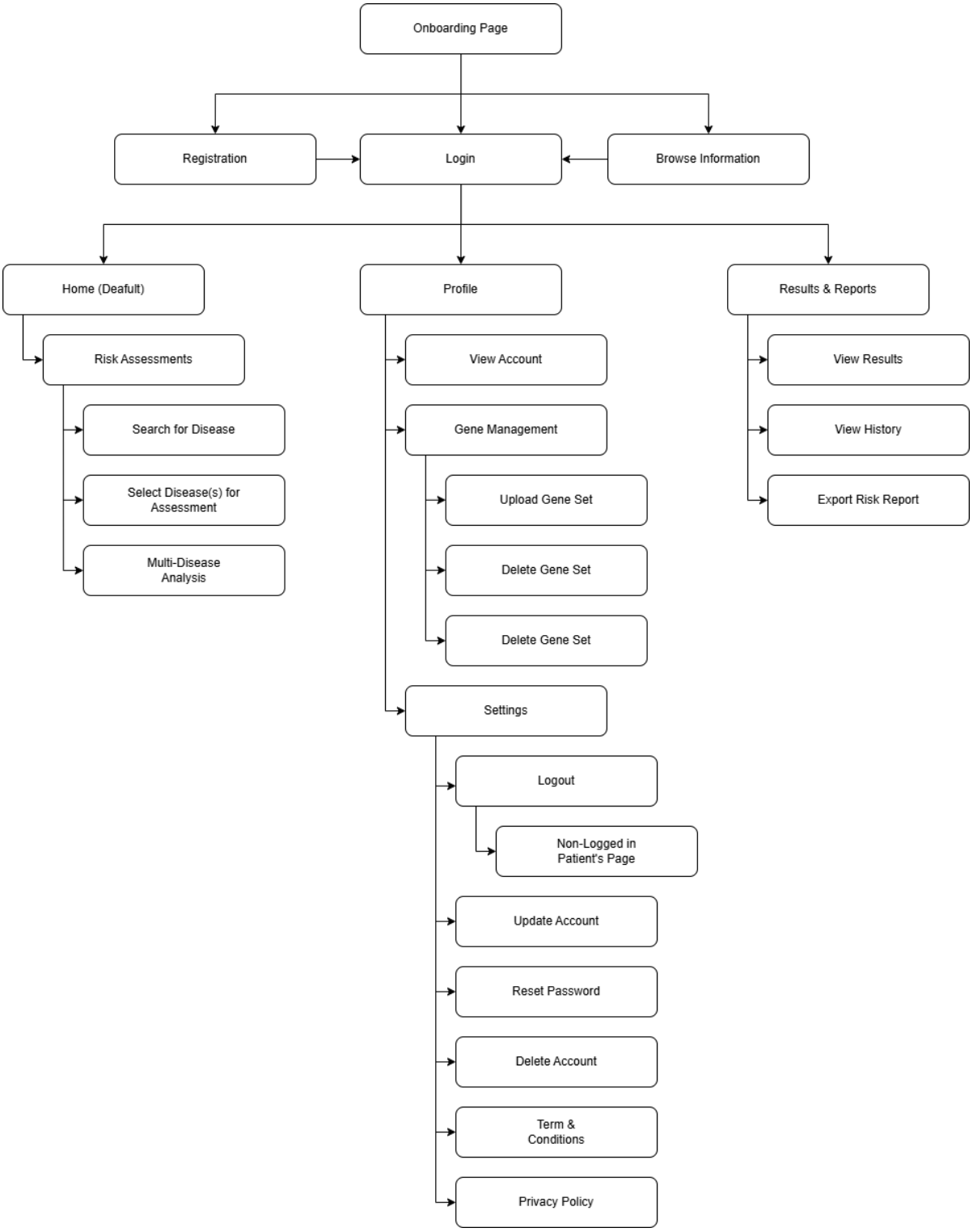
6.2.1 Work Breakdown Structure



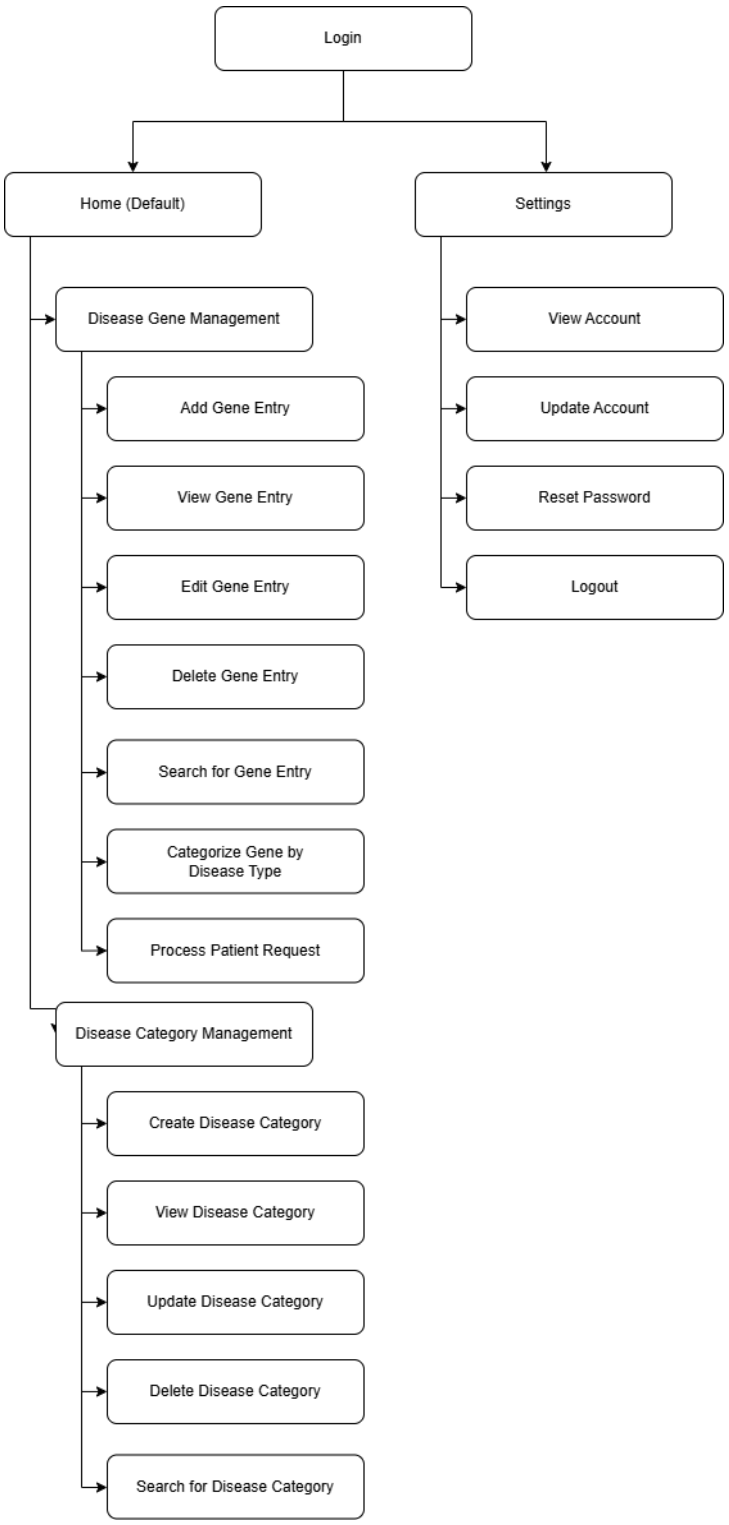
6.2.2 Non-Logged Page



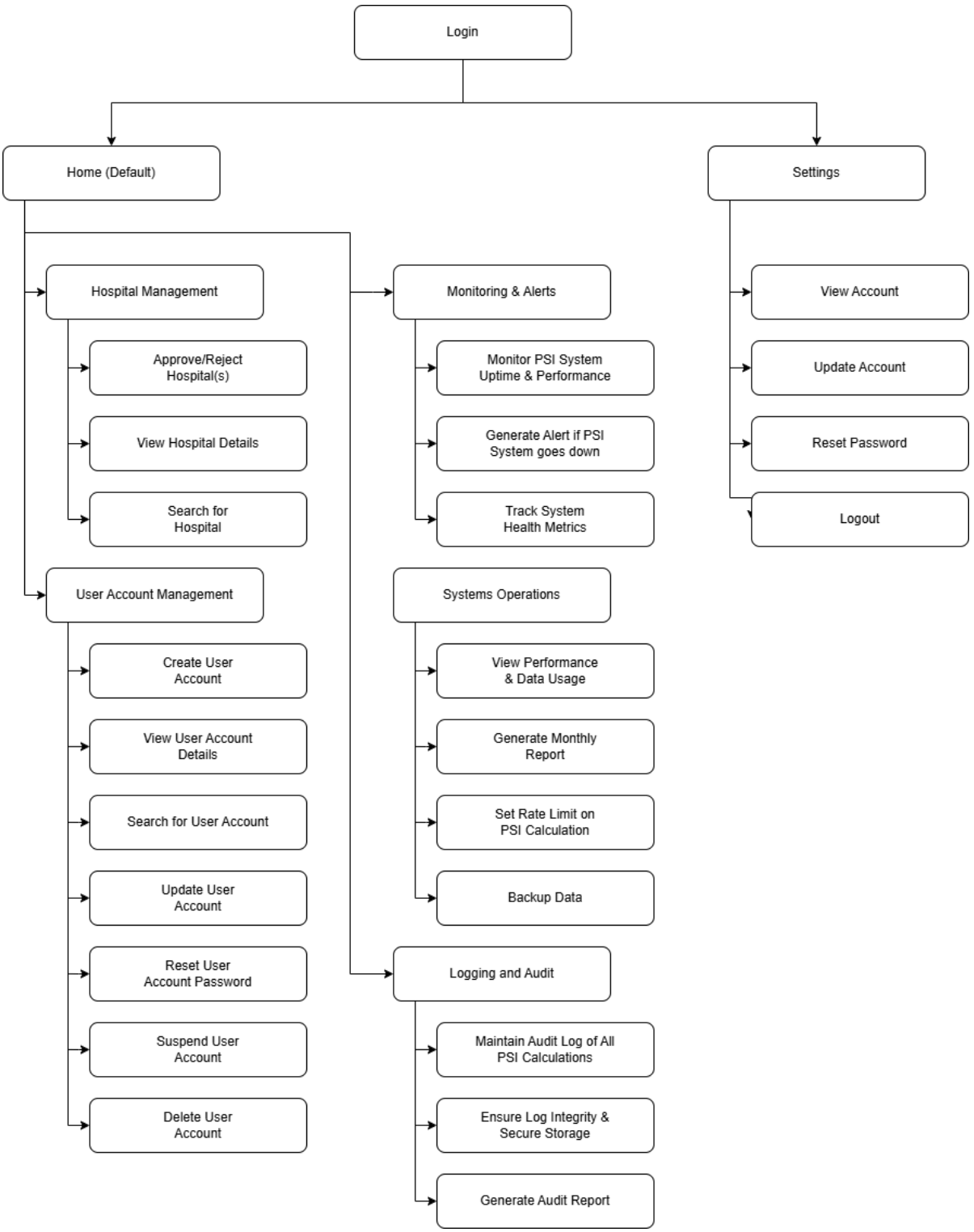
6.2.3 Patients



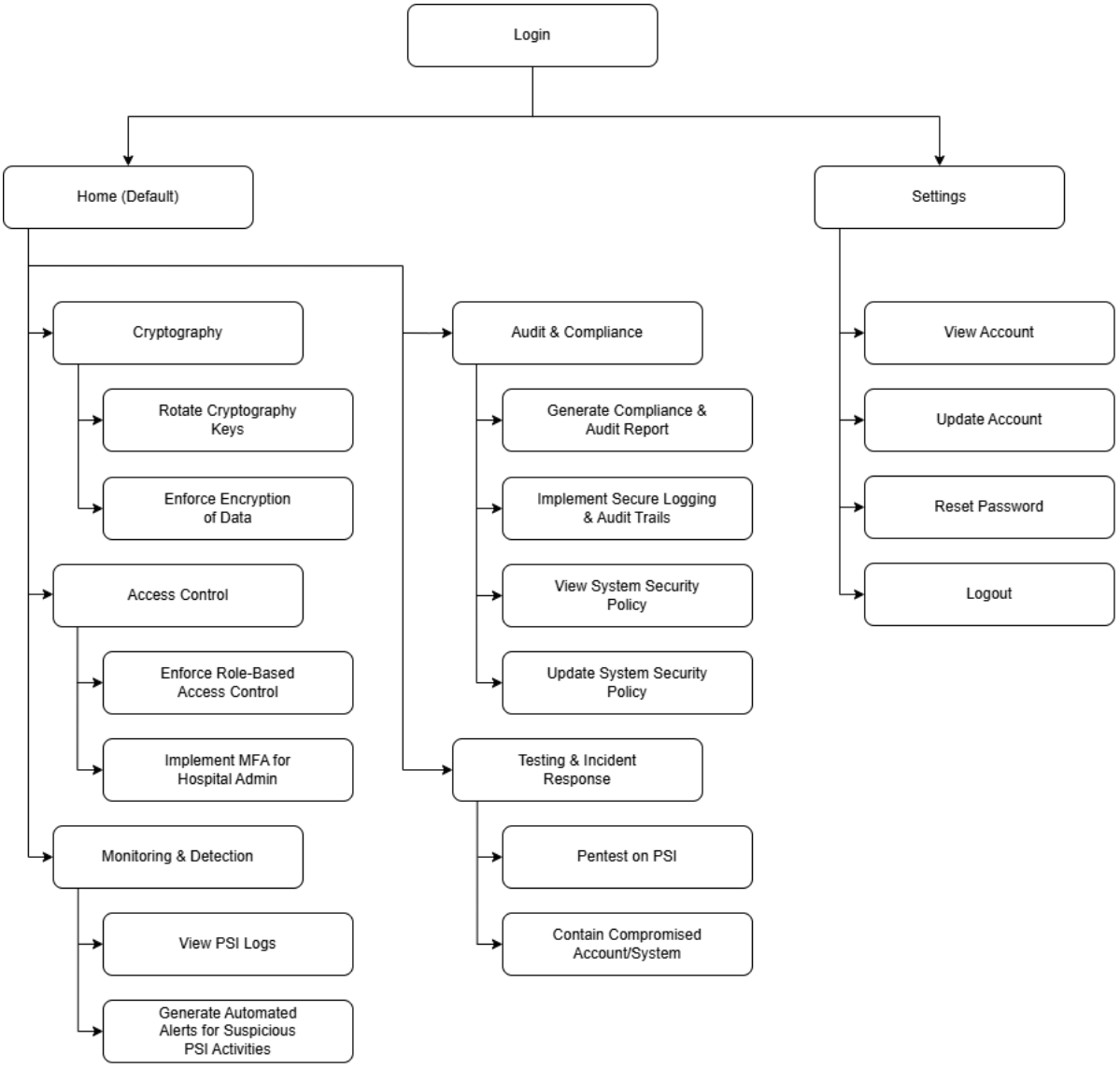
6.2.4 Hospital/Healthcare Provider



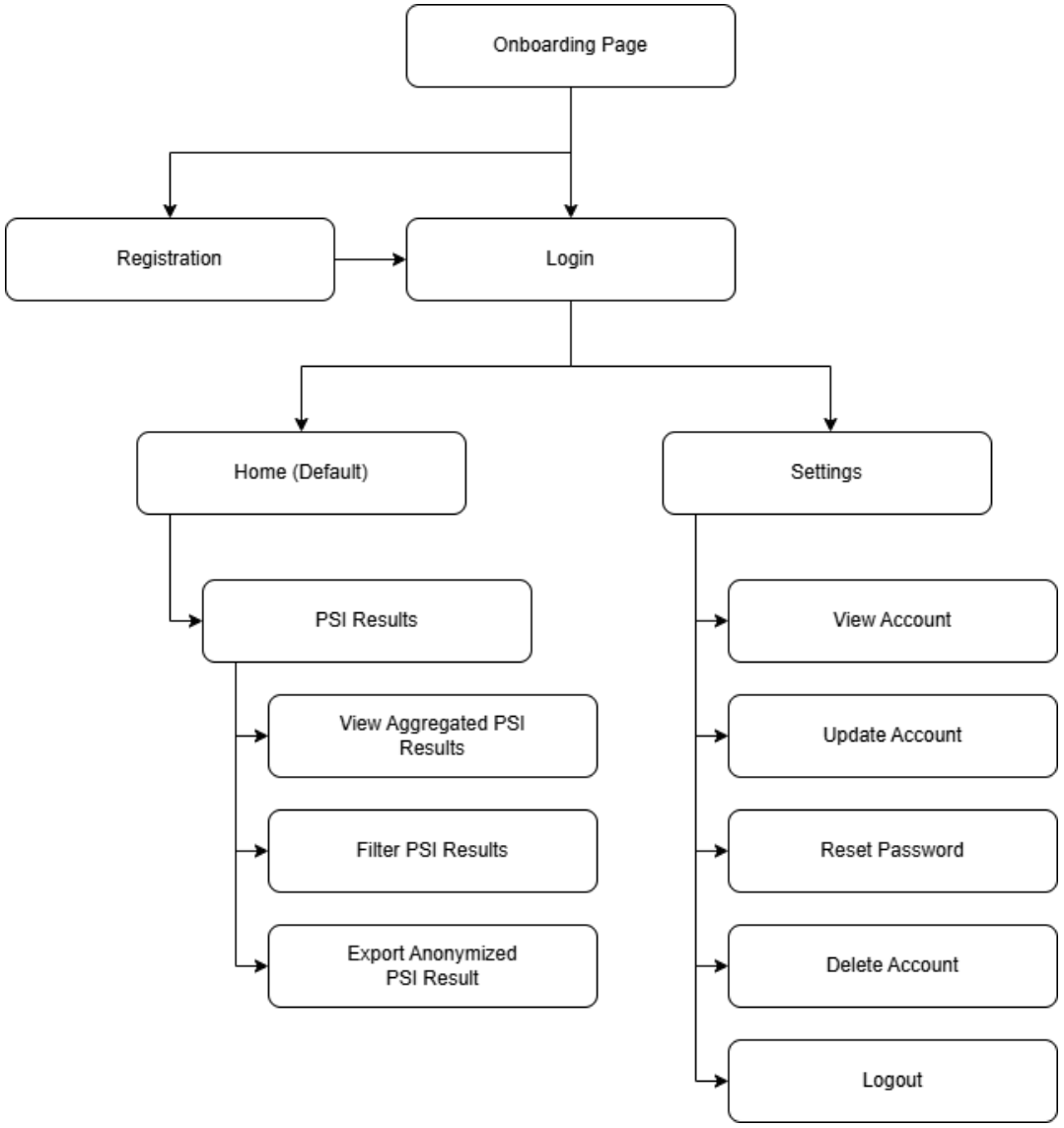
6.2.5 System Administrator



6.2.6 System Security



6.2.7 Health Researcher



6.3 Project Vision

To become the leading global platform for privacy-preserving healthcare data collaboration, enabling secure genetic risk assessments and medical research that protects patient privacy while advancing medical science and improving patient outcomes worldwide.

Our vision encompasses:

Vision		
1.	Privacy First	Establishing the gold standard for privacy-preserving healthcare applications.
2.	Global Impact	Enabling international healthcare collaboration while maintaining data sovereignty.
3.	Patient Empowerment	Giving patients control over their genetic information and disease risk insights.
4.	Research Advancement	Accelerating medical research through secure data sharing without compromising privacy.
5.	Trust and Transparency	Building trust through cryptographic guarantees rather than just policies.

6.4 Project Goals

8 following goals have been established for the successful completion of this project:

Goals		
1.	Successful Development Within Timeline	Complete all phases of development and deliver a fully functional product by the established project deadline.
2.	Meet Scope Requirements	Deliver all features and capabilities as defined in the project scope, including patient risk assessment, hospital gene management, researcher collaboration, and system administration.
3.	Achieve Security and Compliance Standards	Successfully implement and validate PSI protocols, encryption mechanisms, and achieve compliance with healthcare data protection regulations (HIPAA, GDPR, PDPA).

4.	Demonstrate Technical Feasibility	Prove that PSI-based genetic risk assessment is computationally feasible, accurate, and scalable for real-world healthcare applications.
5.	Achieve Stakeholder Approval	Obtain approval from project assessors, supervisors, and potential healthcare partners for system design, implementation, and security measures.
6.	User Acceptance and Usability	Achieve positive feedback from user acceptance testing, demonstrating that the system is intuitive, reliable, and meets user needs across all roles.
7.	Documentation Excellence	Produce comprehensive technical documentation, user manuals, and system administration guides that enable future maintenance and expansion.
8.	Establish Foundation for Future Expansion	Create a modular, scalable architecture that allows for future enhancements such as additional disease categories, advanced analytics, and integration with external healthcare systems.

6.5 Project Risk Analysis

The following risks have been identified and mitigation strategies have been developed:

Risk	Likelihood	Severity	Impact	Mitigation Strategy
Security Vulnerability (Data Breach, PSI Protocol Flaw)	Medium	High	Exposure of sensitive genetic data Loss of patient trust Legal and regulatory consequences	Implement end-to-end encryption Conduct regular security audits and penetration testing Use proven cryptographic libraries Implement multi-factor authentication
PSI Computation	Medium	High	Slow risk assessment results	Optimize PSI algorithm implementation

Performance Issues			Poor user experience System scalability issues	Conduct performance testing early Use cloud auto-scaling Implement caching strategies
Data Privacy Compliance Failure	Low	High	Legal penalties and fines Cannot operate in certain regions Reputational damage	Engage legal/compliance experts early Build compliance into design Document all data handling procedures Conduct compliance audits
Inaccurate Risk Calculation	Medium	High	Incorrect patient risk assessments Loss of credibility Potential harm to patients	Validate PSI algorithm with test datasets Work with medical experts to verify calculations Implement extensive testing Include disclaimers and recommendations for professional consultation
Failure to Meet Deadline	Medium	High	Incomplete deliverables Project failure	Create detailed project schedule with milestones Conduct weekly progress reviews Maintain task tracking system Build in buffer time for unexpected issues
Scope Creep	High	High	Delayed timeline Increased workload Core features compromised	Define clear project scope and requirements Establish change control process Prioritize must-have vs nice-to-have features

				Regular stakeholder communication
Team Member Unavailability	Medium	Medium	Delayed tasks Knowledge gaps	Cross-train team members Maintain comprehensive documentation Use version control for all work Have backup resources identified
Technical Complexity Underestimation	High	Medium	Longer development time Potential technical debt	Conduct thorough technical research early Build proof-of-concept for complex features Seek expert consultation when needed Iterate in small increments
Integration Issues with External Systems	Low	Medium	Delayed deployment Reduced functionality	Design for modularity and loose coupling Use standard APIs and protocols Test integrations early and often Have fallback options for critical integrations

7 Project Plan

7.1 Software Development Methodology

Our team evaluated several software development methodologies for this project including Waterfall, Kanban, and Scrum. After careful consideration of the project's requirements and constraints, the team selected the Agile Scrum methodology as the most suitable approach for the PSI Healthcare Application development.

The decision to adopt Scrum was based on several key factors:

Flexibility and Adaptability: Unlike the Waterfall methodology, which follows a rigid sequential approach with minimal room for changes once a phase is complete, Scrum allows our team to adapt to the ever evolving requirements. Given the complex nature of implementing Private Set Intersection protocols and healthcare compliance standards, the ability to incorporate feedback and make iterative improvements is crucial.

Iterative Development: Scrum's sprint-based approach enables us to deliver functional increments of the system regularly. This is particularly important for our project, as we need to validate the PSI protocol implementation, security measures, and user interface designs progressively throughout development rather than waiting until the end.

Frequent Stakeholder Engagement: The Scrum framework emphasizes regular communication with stakeholders through sprint reviews and demonstrations. For a healthcare application dealing with sensitive genetic data, continuous validation with our supervisor, security personnel, and potential users is essential to ensure the system meets all security, privacy, and usability requirements.

Risk Mitigation*:* By developing in short sprints (typically a week or two depending on the assigned workload), we can identify and address technical challenges, security vulnerabilities, and integration issues early in the development process. This is particularly critical for implementing cryptographic PSI protocols and ensuring HIPAA, GDPR, and PDPA compliance.

Clear Time Frames: While Kanban offers continuous flow without fixed timeframes, Scrum provides structure sprints with defined start and end dates. This structure aligns well with our project deadlines and assessment requirements, allowing us to plan deliverables systematically and track progress against the project timeline.

Team Collaboration: Scrum promotes daily stand-ups, sprint planning, and retrospectives, which enhance team communication and coordination. Given the technical complexity of implementing PSI protocols alongside web application development, strong collaboration is essential for success.

Throughout the project, we will conduct sprint planning sessions to define tasks, hold daily stand-ups to synchronize team efforts, conduct sprint reviews to demonstrate progress, and perform sprint retrospectives to continuously improve our development process.

7.2 Project Deliverables

No	Title	Description	Deadline
1	Project Requirements Documentation	To document the information collected regarding the project's requirements, including system features, functionality, constraints, and project objectives. This includes functional requirements for all user roles (patients, hospitals, researchers, administrators, security personnel), non-functional requirements (security, performance, scalability), PSI protocol specifications, and compliance requirements for healthcare data protection regulations.	Week 5 8 November 2025 9:00 PM Singapore time
2	Project Progress Report: Preliminary Technical Documentation and Preliminary User Manual	To deliver preliminary technical documentation describing the system architecture, PSI protocol implementation approach, database design, and security measures. The preliminary user manual will provide initial guidance for different user roles. Progress report will document work completed, current development status, and upcoming tasks.	Week 10 13 December 2025 9:00 PM Singapore time
3	Project Progress Presentation – Prototype Demo	To present a working prototype demonstrating core functionality of the PSI Healthcare Application, including user interface designs, PSI computation capabilities, patient risk assessment workflow, and hospital gene database management features.	Week 11 20 December 2025 9:00 PM Singapore time
4	Final Product and Documentation	To deliver the complete PSI Healthcare Application including: Source Code, Final Technical Documentation, User Manual,	Week 19 14 February 2026

		Testing Documentation, Project Video, Marketing Video (1-2 minutes), Final Website, Peer Assessment, and Review by Supervisor.	9:00 PM Singapore time
5	Reflective Diary	To compile individual weekly reflections documenting each team member's contributions, challenges, and learning throughout the project.	Week 19 14 February 2026 9:00 PM Singapore time (Final combined submission)
6	Final Presentation	To deliver a comprehensive presentation (approximately 30 minutes) demonstrating the completed application and explaining implementation details.	Week 20 21 February 2026 9:00 PM Singapore time
7	Final Online Submission to SIM	To submit all final documentation and materials to SIM for archival and assessment.	28 February 2026 9:00 PM Singapore time

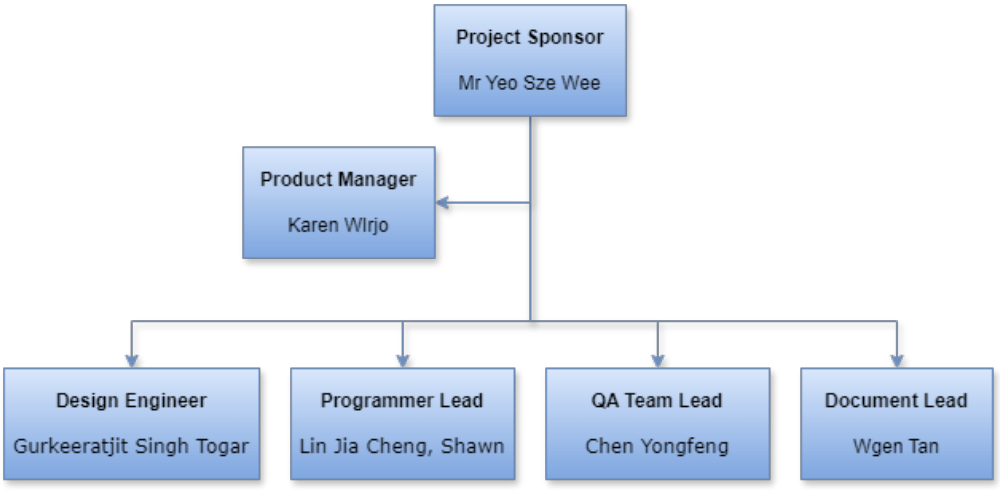
7.3 Reporting Plan

Our team primarily communicates and coordinates through Telegram messaging for day-to-day discussions, questions, and quick updates. In-person team meetings are scheduled as needed when all members are available to meet. These meetings focus on major decisions, sprint planning, and sprint retrospectives to ensure effective collaboration and continuous improvement throughout the project lifecycle.

Formal supervisor meetings are held every two weeks (fortnightly) to review the team's progress, discuss any challenges or roadblocks, and obtain guidance on technical implementation and project direction. These meetings may be conducted via online or in-person at SIM, depending on availability and scheduling. The agenda for supervisor meetings typically includes project progress updates, demonstration of completed features or prototypes, discussion of technical challenges related to PSI implementation, review of upcoming sprint goals, and clarification of requirements or scope adjustments.

Report	Description
Meeting Time	It will be recorded in a document during every supervisor meeting and submitted to the project supervisor. Meeting Time will capture key decisions, action items, technical discussions, and any requirement changes agreed upon during the meeting.
Weekly Progress Report (Reflective Diary)	Each team member will write and submit a personal reflective diary entry every week (due Sunday) to the project supervisor. The reflective diary documents individual contributions, challenges encountered, lessons learned, time spent on various tasks, and personal reflections on the project progress. This serves as both a self-assessment tool and a record of individual effort throughout the project lifecycle.

7.4 Proposed Project Organisation



7.4.1 Roles & Responsibilities

Roles	Responsibilities
Project Sponsor	Supervise overall project execution. Guide team on technical specifications and implementation approach.
Product Manager	Coordinate and monitor project deliverables and milestones. Organize team meetings in coordination with supervisor and sponsor. Report progress updates to the project sponsor.
Design Engineer	Create product designs and deliverables. Investigate and propose design methodologies. Validate usability of product interfaces. Conduct testing and evaluation of prototypes.
Programmer Lead	Supervise development activities and coding progress. Select appropriate programming technologies and frameworks. Implement application functionality.
QA Team Lead	Design and execute test scenarios for system validation.

	Document and communicate defects to Programmer Lead. Verify compliance with defined project specifications.
Document Lead	Oversee all project documentation activities. Conduct background research for project materials. Track milestone completion against project timeline.

7.4.2 Roles & Responsibilities Matrix

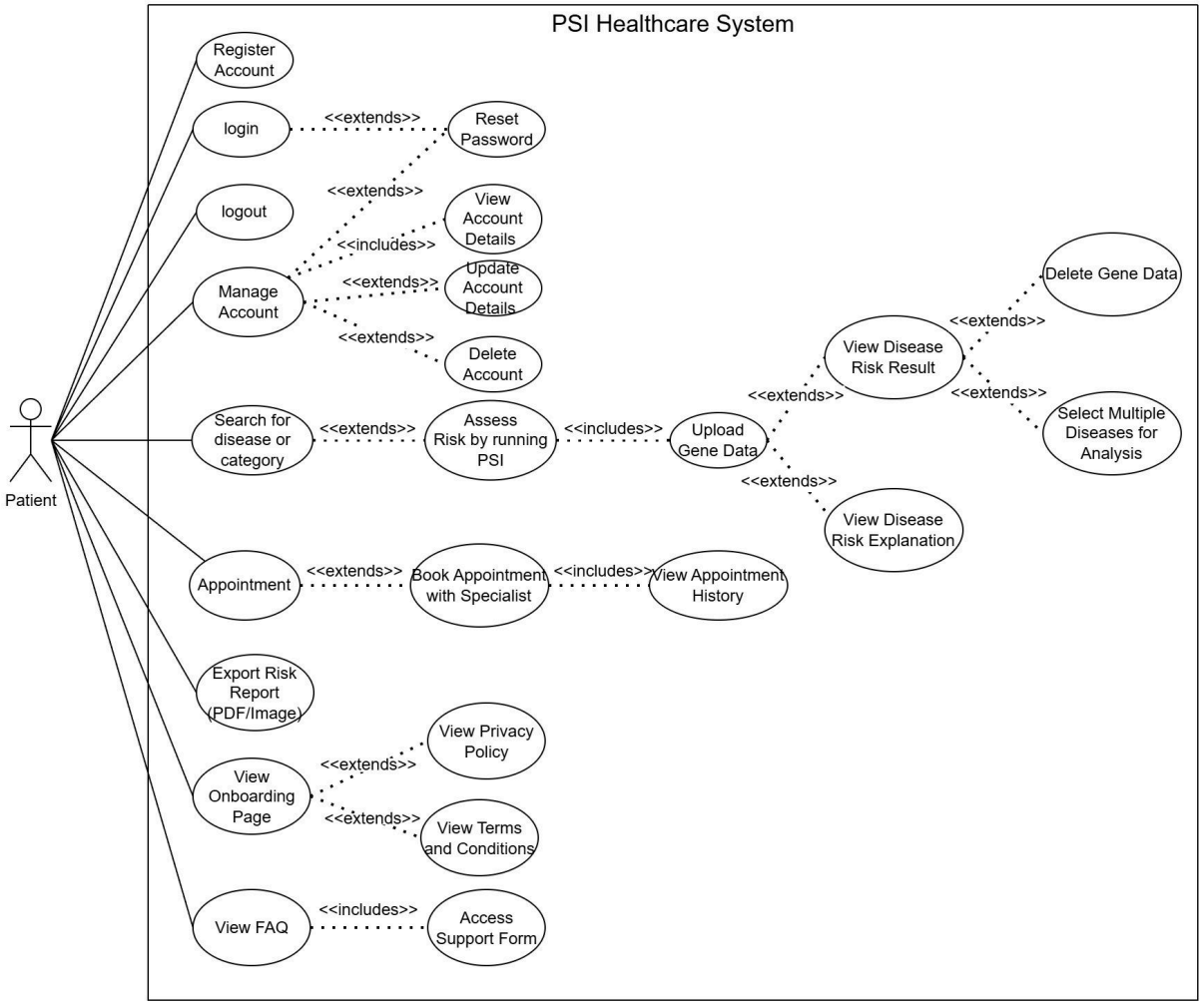
Name	Karen Wirjo	Gurkeeratjit Singh Togar	Lin Jia Cheng, Shawn	Chen Yongfeng	Wgen Tan
Roles	**Product Manager**	**Design Engineer**	**Programmer Lead**	**QA Team Lead**	**Document Lead**
Project Leader	✔				
Wireframe		✔			
Prototype Design		✔			
Frontend developer	✔	✔	✔	✔	
Backend developer	✔		✔		
Documentation	✔	✔	✔	✔	✔
Testing				✔	

8 Product Requirements Specification

8.1 Functional Requirements

8.1.1 Patient

8.1.1.1 Use Case Diagram



8.1.1.2 User Stories

No.	Patient User Stories
1	As a patient, I want to be able to register for an account with my email and password, so that I can securely access the disease risk assessment system.
2	As a patient, I want to login to my account,so that I can securely access the genetic data and assessment results.
3	As a patient, I want to logout of my account,so that I can maintain the security

	and privacy of my account.
4	As a patient, I want to reset my password if I forget it, so that I can regain access to my account without losing my data.
5	As a patient with genetic test results, I want to securely upload my gene set to initiate a PSI-based risk assessment, so that I can learn my disease risk percentage without revealing my entire genetic profile.
6	As a patient, I want the results to be presented in a simple way,so that I can easily and accurately understand my risk of having a particular disease.
7	As a patient, I want to receive my risk assessment as a clear percentage (e.g, “15% increased risk”), so that I can understand the likelihood of developing the disease.
8	As a patient, I want to receive a clear explanation of what my risk percentage means,so that I understand the basis of my result and what actions to consider next.
9	As a patient, I want to be able to delete my gene data from the system after getting results, so that I maintain control over my personal genetic information.
10	As a patient, I want to view the history of my past genetic assessments and actions taken for different diseases,so that I can track how my risk profile changes over time or across different conditions.
11	As a patient, I want to have the option to select and analyse my risk for multiple diseases in a single session, so that I can efficiently assess my genetic predisposition to various conditions without repeating the upload process.
12	As a patient, I want to export my risk assessment results out as either an image or a pdf report,so that I can save/share them across different devices/people.
13	As a patient, I want to view my account details, so that I can verify my personal information is accurate and up to date.
14	As a patient, I want to update my account information (email, contact details, password), so that I can keep my profile current and maintain secure access to the system.
15	As a patient, I want to delete my account permanently, so that I can remove my personal data from the system and reduce privacy risks when I no longer need the service.
16	As a Patient, I want to browse the information about the genetic risk assessment and PSI protocol, so that I can understand the services provided before deciding to register.

17	As a Patient, I want to view public resources about genetic diseases and risk factors, so that I can learn about the health conditions without needing an account
18	As a Patient, I want to access contact information or support form, so that I can make enquiries before deciding to register
19	As a Patient, I want to view frequently asked questions, so that I can get answers to common questions without needing to contact support
20	As a Patient, I want to view unlogged main page, so that I can know what information I have access to without an account
21	As a Patient, I want to view onboarding page, so that I can understand how to use the platform before creating an account
22	As a Patient, I want to view the privacy policy, so that I can understand how my personal data is collected, used and protected
23	As a Patient, I want to view the terms and conditions, so that I can understand the rules for using the app
24	As a patient, I want to search for specific diseases or categories, so that I can quickly find the risk assessments most relevant to me.

8.1.1.3 Use Case Description

Name:Register Account (Patient)	**ID: P01**
Stakeholders and goals: Patients want to register for an account so they can securely access the PSI system.	
Description: Allows new patients to create an account using their email and password to access healthcare risk assessment services.	
Actors: Patient	
Trigger: The patient selects the “Register” option on the login page.	
Normal Flow: 1. The patient clicks on “Register”. 2. The system prompts for email and password. 3. The system validates the input. **4.** The account is created and confirmation is sent to the patient.	
Sub-Flows: Email verification process.	

Alternative/Exceptional Flows:

- If the email is already in use, the system displays an error message and requests a different email.
- If the entered password and password confirmation do not match, display an error message informing users that the two passwords do not match.
- If the entered passwords match but do not meet the password requirements, display an error message informing users of the password requirements.

Name: Login to Patient Account	**ID: P02**
Stakeholders and goals: Patients want to log in to securely access their data.	
Description: Allows registered patients to log in using valid credentials.	
Actors: Patient	
Trigger: When the patient clicks on “Login.”	
Normal Flow: 1. The patient enters an email and password. 2. The patient clicks “Submit”. 3. The system validates credentials. 4. The system grants access and loads the dashboard.	
Sub-Flows: Session management.	
Alternative/Exceptional Flows: If credentials are invalid, display “Incorrect email or password.”	

Name: Logout from Patient Account	**ID: P03**
Stakeholders and goals: Patients want to log out to maintain account security.	
Description: Ends the user session and redirects the patient to the homepage.	
Actors: Patient	
Trigger: Patient clicks “Logout.”	

Normal Flow: 1. The patient clicks logout. 2. The system ends the active session. 3. The system redirects to the login page.
Sub-Flows: Session termination
Alternative/Exceptional Flows: None

Name: Reset Patient Account Password	**ID: P04**
Stakeholders and goals: Patients want to regain access when they forget their password.	
Description: Allows patients to reset their password securely through their registered email.	
Actors: Patient	
Trigger: Patient clicks “Forgot Password.”	
Normal Flow: 1. The patient requests a password reset. 2. The system prompts for registered email. 3. The system sends a reset link to the email. 4. The patient sets a new password. 5. The system confirms password change.	
Sub-Flows: Email verification and token validation.	
Alternative/Exceptional Flows: If the email is not registered, show “Account not found.”	

Name: Upload Gene Data	**ID: P05**
Stakeholders and goals: Patients want to upload genetic data for private risk assessment.	
Description: Enables patients to securely upload their genetic data file for PSI comparison with hospital datasets.	

Actors: Patient
Trigger: Patient clicks “Upload Gene Data.”
Normal Flow: 1. The patient selects a gene data file. 2. The system validates file type and size. 3. The system encrypts the file and initiates PSI processing. 4. The system confirms upload success.
Sub-Flows: Encryption and file validation.
Alternative/Exceptional Flows: If file format is invalid, show error and prompt re-upload.

Name: View Risk Result in Simple Format	**ID: P06**
Stakeholders and goals: Patients want easily understandable results.	
Description: Displays PSI computation results clearly using visuals or text indicators.	
Actors: Patient	
Trigger: System completes PSI analysis.	
Normal Flow: 1. The system generates output. 2. The patient views a simple summary.	
Sub-Flows: None	
Alternative/Exceptional Flows: If computation fails, message: “Result unavailable.”	

Name: View Disease Risk Explanation	**ID: P07**
Stakeholders and goals: Patients want to understand their risk result meaning.	
Description: Provides an easy-to-understand explanation of the disease risk percentage.	
Actors: Patient	

Trigger: Patient clicks “View Explanation.”
Normal Flow: 1. The patient clicks the “View Explanation” button. 2. The system loads explanatory text and possible next steps. 3. The patient reads the loaded explanation.
Sub-Flows: Information retrieval
Alternative/Exceptional Flows: If explanation is unavailable (eg. cannot be found, no explanation provided), show “No details found.”

Name: View Explanation of Risk Percentage	**ID: P08**
Stakeholders and goals: Patients want to understand what their PSI-generated risk percentage means, including its interpretation and recommended next steps.	
Description: After the Private Set Intersection (PSI) process generates a disease risk percentage, the system provides an explanation of how the result was derived and what it implies for the patient’s health. This includes contextual information such as comparison with population averages and suggested follow-up actions.	
Actors: Patient	
Trigger: The patient clicks or taps the “View Explanation” or “Learn More” option after receiving their PSI risk result.	
Normal Flow: 1. The system retrieves the explanation related to the patient’s calculated risk percentage. 2. The explanation includes a brief interpretation of the result (e.g., “15% increased risk compared to average population”). 3. The system displays general health recommendations or advises consulting a medical professional for further guidance. 4. The patient reads and acknowledges the explanation.	
Sub-Flows: The system may include visual aids such as charts or color-coded indicators (e.g., low, moderate, high risk).	
Alternative/Exceptional Flows: If the explanation data cannot be retrieved, the system displays a message: “Explanation temporarily unavailable. Please try again later.”	

Name: Delete Gene Data	ID: P09
Stakeholders and goals: Patients want to delete their uploaded genetic data for privacy.	
Description: Allows patients to permanently delete stored genetic data from the database.	
Actors: Patient	
Trigger: Patient clicks “Delete Data.”	
Normal Flow: 1. The patient selects the file or dataset to delete. 2. The system asks for confirmation. 3. The system deletes encrypted files from storage. 4. The system confirms deletion success.	
Sub-Flows: Confirmation dialog.	
Alternative/Exceptional Flows: If deletion fails, show “Unable to delete data.”	

Name: View History of Past Assessments	ID: P10
Stakeholders and goals: Patients want to track their results over time..	
Description: Displays all past PSI analyses and outcomes.	
Actors: Patient	
Trigger: Patient selects “Assessment History.”	
Normal Flow: 1. The system retrieves stored results. 2. Patient views a list of past assessments.	
Sub-Flows: None	
Alternative/Exceptional Flows: If no past data, system displays “No records found.”	

Name: Select Multiple Diseases for Analysis	ID: P11
Stakeholders and goals: Patients want to analyze multiple diseases in one	

session.
Description: Allows patients to select multiple disease categories for PSI computation.
Actors: Patient
Trigger: Patient selects multiple diseases from dropdown or checklist.
Normal Flow: 1. The patient chooses diseases to assess. 2. The system runs PSI processes for each selected disease. 3. Results are aggregated and shown together.
Sub-Flows: Parallel PSI execution - Allows user to run PSI algorithm for multiple diseases at the same time
Alternative/Exceptional Flows: If one dataset fails, the system continues with remaining selections.

Name: Export Assessment Results	**ID: P12**
Stakeholders and goals: Patients want to save or share results.	
Description: Allows exporting PSI results as image or PDF report.	
Actors: Patient	
Trigger: Patient selects “Export Results.”	
Normal Flow: 1. The system generates downloadable files. 2. Patient saves report locally.	
Sub-Flows: None	
Alternative/Exceptional Flows: If export fails, message: “Export unsuccessful.”	

Name: View Account Details	**ID: P13**
Stakeholders and goals: Patients want to verify that their stored account information (e.g., name, email, contact details) is correct and up to date.	
Description: Displays the patient’s registered account information in a read-only format so they can confirm its accuracy and ensure their details are correctly	

recorded in the system.
Actors: Patient
Trigger: The patient selects “My Account” or “View Account Details” from the user menu.
Normal Flow: 1. The system authenticates the patient’s session. 2. The system retrieves the patient’s profile details from the database. 3. The details (name, email, contact number, registration date, etc.) are displayed on the screen. 4. The patient reviews their information
Sub-Flows: The system may include an option to navigate to “Update Account Information” for edits.
1. **Alternative/Exceptional Flows:** If account data cannot be retrieved, the system displays an error message: “Unable to load account details. Please refresh or try again later.” 2. If the session expires, the system prompts the user to log in again.

Name: Update Account Information	**ID: P14**
Stakeholders and goals: Patients want to keep their contact and login details accurate for secure access.	
Description: Allows patients to modify personal details such as email, contact number, or password. Actors: Patient	
Actors: Patient	
Trigger: Patient selects “Edit Profile” option from account settings.	
Normal Flow: 1. The patient enters new account information. 2. The system validates input (e.g., email format, password strength). 3. Updated details are saved successfully. 4. Confirmation message displayed.	

Sub-Flows: None
Alternative/Exceptional Flows: If validation fails, system shows error message and requests correction.

Name: Delete Account Permanently	**ID: P15**
Stakeholders and goals: Patients want control over their personal data and privacy.	
Description: Enables patients to permanently delete their account and all associated data.	
Actors: Patient	
Trigger: Patient selects “Delete Account.”	
Normal Flow: 1. The system prompts for confirmation. 2. The patient confirms deletion. 3. The system removes patient data securely. 4. The system displays a confirmation message.	
Sub-Flows: None	
Alternative/Exceptional Flows: If patient cancels, deletion process stops.	

Name: View Information About Genetic Risk Assessment and PSI Protocol	**ID: P16**
Stakeholders and goals: Patients want to understand how the PSI-based assessment works before registering.	
Description: Displays educational content about the PSI system, how data is handled, and what users can expect from the genetic risk analysis.	
Actors: Patient (Unregistered or Registered)	
Trigger: User clicks “Learn About PSI.”	
Normal Flow: 1. System retrieves and displays overview content on PSI and its benefits. 2. The patient reviews the material.	

Sub-Flows: None
Alternative/Exceptional Flows: If content fails to load, an error message appears.

Name: View Public Resources About Genetic Diseases and Risk Factors	**ID: P17**
Stakeholders and goals: Patients want to learn about health conditions before using the PSI service.	
Description: Provides access to general information and educational resources about genetics and disease risks.	
Actors: Patient (Unregistered)	
Trigger: User selects “Public Resources” or “Learn More.”	
Normal Flow: 1. The system retrieves articles or links from the database. 2. The patient browses topics by category.	
Sub-Flows: None	
Alternative/Exceptional Flows: If resources are unavailable, system shows “No content available.”	

Name: Access Contact Information or Support Form	**ID: P18**
Stakeholders and goals: Patients want to make inquiries or request assistance before signing up.	
Description: Provides hospital or platform contact details and a form for submitting questions.	
Actors: Patient(Unregistered)	
Trigger: User selects “Contact Support.”	
Normal Flow: 1. The system displays contact details and/or support form. 2. Patient submits inquiry. 3. Confirmation message displayed.	
Sub-Flows: None	

Alternative/Exceptional Flows: If submission fails, the system displays an error message.

Name: View Frequently Asked Questions (FAQ)	**ID: P19**
Stakeholders and goals: Patients want quick answers without contacting support.	
Description: Displays categorized FAQ section addressing common issues or queries about the PSI platform.	
Actors: Patient (Unregistered)	
Trigger: User selects “FAQ.”	
Normal Flow: 1. System retrieves FAQ data. 2. Patient browses or searches by keyword.	
Sub-Flows: None	
Alternative/Exceptional Flows: If no FAQs are available, the system displays “No questions found.”	

Name: View Unlogged Main Page	**ID: P20**
Stakeholders and goals: Patients want to explore basic platform information before creating an account.	
Description: Displays the homepage and general features accessible to all visitors.	
Actors: Patient (Unregistered)	
Trigger: User accesses the main website.	
Normal Flow: 1. The system loads homepage content and navigation links. 2. Patients can explore available sections such as PSI info or registration.	
Sub-Flows: None	
Alternative/Exceptional Flows: If page fails to load, system prompts to refresh.	

Name: View Onboarding Page	ID: P21
Stakeholders and goals: Patients want clear instructions before using the platform.	
Description: Provides a walkthrough or guide explaining how to register, upload genetic data, and interpret PSI results.	
Actors: Patient (Unregistered)	
Trigger: User clicks “Getting Started” or “How It Works.”	
Normal Flow: 1. The system loads onboarding steps. 2. The patient follows visual guide or instructions.	
Sub-Flows: None	
Alternative/Exceptional Flows: If content is not found, the system shows “Guide unavailable.”	

Name: View Privacy Policy	ID: P22
Stakeholders and goals: Patients want to understand how their personal and genetic data is used and protected.	
Description: Displays the platform’s privacy policy outlining data collection, processing, and sharing rules.	
Actors: Patient / Public User	
Trigger: User clicks “Privacy Policy.”	
Normal Flow: 1. The system retrieves privacy policy documents. 2. The patient reads policy content.	
Sub-Flows: None	
Alternative/Exceptional Flows: If document not found, display “Policy temporarily unavailable.”	

Name: View Terms and Conditions	ID: P23
Stakeholders and goals: Patients want to understand platform usage rules before registering.	

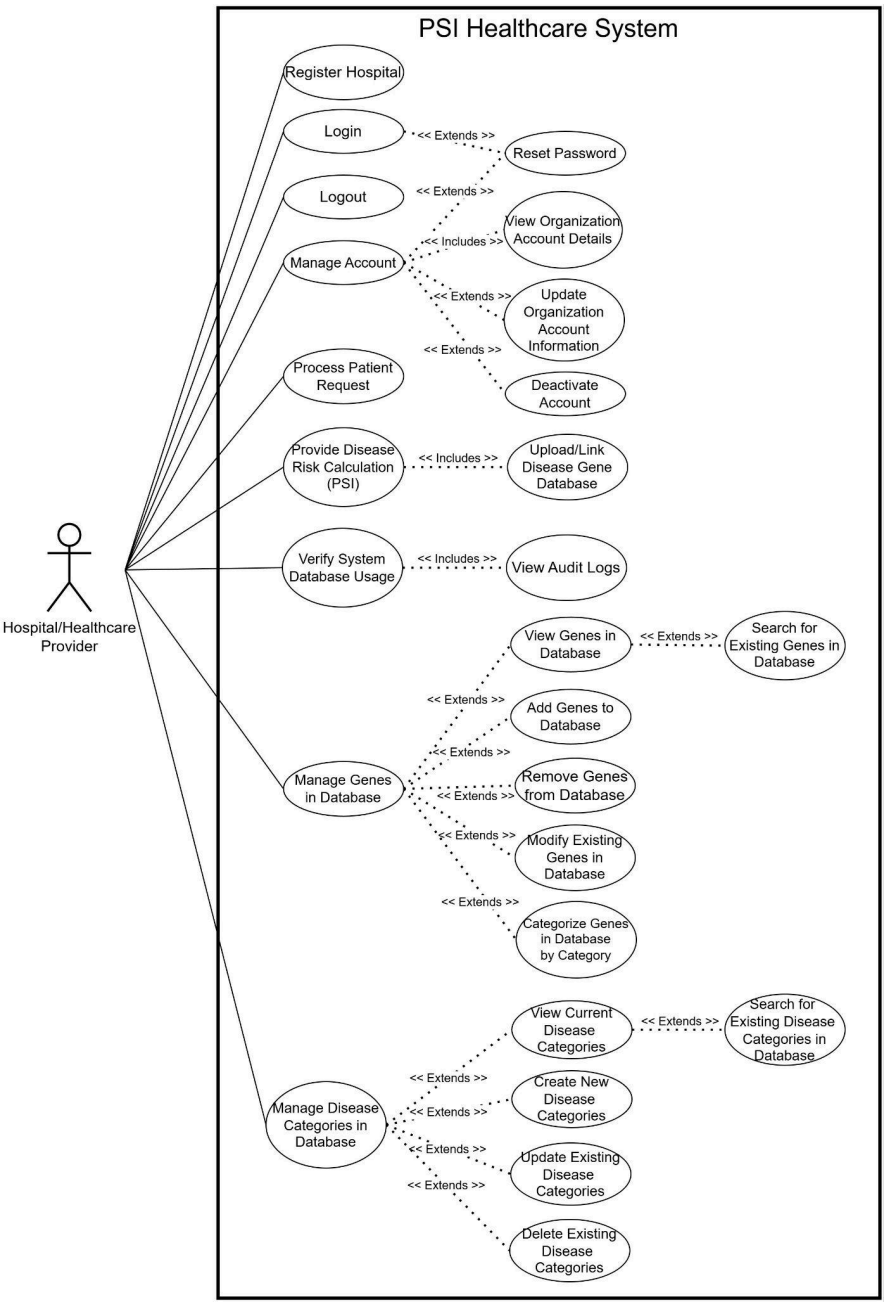
Description: Displays the platform's terms of use and legal agreements.
Actors: Patient / Public User
Trigger: User clicks "Terms and Conditions."
Normal Flow: 1. The system retrieves terms of service content. 2. The patient reads the document.
Sub-Flows: Historical data retrieval.
Alternative/Exceptional Flows: If a document is not found, the system displays "Terms currently unavailable."

Name: Search for disease or category	**ID: P24**
Stakeholders and goals: Patients want to search for specific diseases or categories so that they can quickly find and access relevant risk assessments.	
Description: Allows the patient to search for diseases or categories in the system to identify and view corresponding risk assessments related to their health concerns.	
Actors: Patient	
Trigger: Patient clicks on the "Search Disease/Category" option in the Risk Assessment section.	
Normal Flow: 1. The patient logs into the system. 2. The patient navigates to the Risk Assessment section. 3. The patient clicks on Search Disease/Category. 4. The system displays a search bar and filter options. 5. The patient enters the name of a disease or category. 6. The system searches the database for matching results. 7. The system displays a list of related diseases or categories along with available risk assessments. 8. The patient selects a result to view the detailed risk assessment information.	

Sub-Flows: Search and filter functions.
Alternative/Exceptional Flows: ● If no matching results are found, the system displays “No matching diseases or categories found.” ● If a database or system error occurs, the system displays an error message and logs the issue.

8.1.2 Hospital/Healthcare Provider

8.1.2.1 Use Case Diagram



8.1.2.2 User Stories

No.	Hospital User Stories
1	As a hospital administrator, I want to register my hospital organization on the platform, so that we can provide disease risk assessment services to patients
2	As a hospital with a disease gene database,I want to securely provide disease risk calculations to patients,so that I can help patients without accessing their private genetic data.
3	As a hospital with a disease gene database, I want to be able to check whether the system is using our disease gene database correctly, so that I can ensure patients receive accurate results based on our research.
4	As a hospital, I want to process multiple patient requests efficiently, so that we can serve many patients without long wait times.
5	As a hospital, I want to add newly discovered disease-associated genes to my database, so that patients can benefit from the latest research findings in their risk assessment.
6	As a hospital, I want to view the disease genes in the database, so that I can view the details of each gene and keep track of what genes are in the database.
7	As a hospital, I want to edit the gene entries in the database (e.g, update risk coefficients or metadata), so that I can correct errors and reflect new research findings.
8	As a hospital administrator, I want to login to my account, so that I can securely access the genetic data.
9	As a hospital administrator, I want to logout of my account, so that I can maintain the security and privacy of my account.
10	As a hospital administrator, I want to reset my password if I forget it, so that I can regain access to my account without losing my data.
11	As a hospital, I want to categorize disease genes by disease type or category (e.g, cardiovascular, oncological, neurological, etc..), so that patients can easily detect which disease risks they want to assess and I can organize my database effectively.
12	As a hospital administrator, I want to view my organization's account details, so that I can verify our registration information is correct.
13	As a hospital administrator, I want to update my organization's account information (contact details, address, administrator credentials), so that I can keep our hospital profile current in the system.

14	As a hospital administrator, I want to deactivate our hospital account if we no longer want to participate in the platform, so that we can cease operations while maintaining data compliance requirements.
15	As a hospital, I want to create new disease categories in my database, so that I can organize newly discovered disease-gene associations.
16	As a hospital, I want to view all disease categories in my database, so that I can see how my genes are organized.
17	As a hospital, I want to update disease category names or descriptions, so that I can keep my classifications current with medical standards.
18	As a hospital, I want to search for specific disease categories, so that I can quickly find and manage categories in large databases.
19	As a hospital, I want to delete unused disease categories, so that I can keep my database clean and organized.
20	As a hospital, I want to search for specific genes in my database, so that I can quickly locate entries for updates or verification.

8.1.2.3 Use Case Description

Name: Register Hospital Organization	**ID: H01**
Stakeholders and goals: Hospitals want to register their organization to participate in PSI-based assessments.	
Description: Allows hospitals to create an official account and submit verification details for approval by the system administrator.	
Actors: Hospital Administrator	
Trigger: Hospital administrator clicks “Register Hospital” on the system homepage.	
Normal Flow: 1. The hospital administrator fills in registration details (name, email, license number, contact info). 2. The system validates and stores details. 3. Request is sent to the system administrator for approval. 4. The hospital receives confirmation once approved.	
Sub-Flows: Admin verification and approval.	

Alternative/Exceptional Flows: If registration data is invalid or incomplete, the system prompts for correction.

Name: Provide Disease Risk Calculation	**ID: H02**
Stakeholders and goals: Hospitals want to process PSI computations to assist patients.	
Description: Enables hospitals to securely contribute their disease gene database to PSI computation without revealing sensitive data.	
Actors: Hospital Administrator	
Trigger: A patient initiates a PSI request.	
Normal Flow: 1. The system sends an encrypted gene set to the hospital PSI engine. 2. The system runs PSI protocol using its disease gene database. 3. Results are returned to the central system.	
Sub-Flows: PSI computation process.	
Alternative/Exceptional Flows: If hospital PSI service is offline, the system retries or selects an alternate provider.	

Name: Verify System Database Usage	**ID: H03**
Stakeholders and goals: Hospitals want to ensure their disease gene database is used correctly.	
Description: Allows hospitals to check how and when their gene data was accessed for PSI operations.	
Actors: Hospital Administrator	
Trigger: Hospital accesses the “Database Logs” page.	
Normal Flow: 1. Hospital logs in. 2. The system displays usage logs showing timestamps, patient requests, and PSI outcomes. 3. Hospital reviews activity.	
Sub-Flows: Log retrieval.	

Alternative/Exceptional Flows: If logs are unavailable, the system shows “No recent activity.”

Name: Process Multiple Patient Requests	**ID: H04**
Stakeholders and goals: Hospitals want to handle multiple PSI computations efficiently.	
Description: Allows hospitals to manage several concurrent patient requests through a queue or batch process.	
Actors: Hospital Administrator	
Trigger: Multiple PSI requests are received.	
Normal Flow: 1. The system adds requests to the processing queue. 2. PSI computations are executed sequentially or in parallel. 3. Results are sent to patients.	
Sub-Flows: Job queue handling.	
Alternative/Exceptional Flows: ● If computation exceeds capacity, the system pauses and notifies the administrator. ● If any request fails, it is flagged for manual review.	

Name: Add New Disease-Associated Genes	**ID: H05**
Stakeholders and goals: Hospitals want to update their gene database with new findings.	
Description: Enables hospitals to add new gene entries with risk factors or associated metadata.	
Actors: Hospital Administrator	
Trigger: Hospital clicks “Add New Gene.”	
Normal Flow: 1. System displays form for new gene entry. 2. Administrator enters gene name, disease type, and coefficient. 3. The system validates and saves entries.	

4. Confirmation is shown.
Sub-Flows: Data validation.
Alternative/Exceptional Flows: If validation fails, show “Invalid gene entry.”

Name: View Disease Gene Database	**ID: H06**
Stakeholders and goals: Hospitals want to review all genes currently stored in their system.	
Description: Allows viewing a list of stored disease-associated genes with details.	
Actors: Hospital Administrator	
Trigger: Hospital administrator clicks “View Gene Database.”	
Normal Flow: 1. The system retrieves all gene entries. 2. Data is displayed in tabular format. 3. Hospital administrators can filter or search entries.	
Sub-Flows: Search and filter functions.	
Alternative/Exceptional Flows: If no data exists, show “No genes in database.”	

Name: Edit Disease Gene Entries	**ID: H07**
Stakeholders and goals: Hospitals want to keep gene information accurate and updated.	
Description: Enables editing existing gene records to correct or update disease relationships.	
Actors: Hospital Administrator	
Trigger: Hospital administrator selects a gene and clicks “Edit.”	
Normal Flow: 1. The system loads gene records for editing. 2. Hospital administrators modify relevant fields. 3. The system saves changes and confirms updates.	

Sub-Flows: Data validation and update.
Alternative/Exceptional Flows: If the record is locked or in use, show “Unable to edit at this moment.”

Name: Login to Hospital Account	**ID: H08**
Stakeholders and goals: Hospitals want secure access to the PSI platform.	
Description: Allows authorized hospital staff to log in with valid credentials.	
Actors: Hospital Administrator	
Trigger: Hospital administrator clicks “Login.”	
Normal Flow: 1. Hospital administrator enters username and password. 2. System verifies credentials. 3. Access granted to the hospital dashboard.	
Sub-Flows: Authentication process.	
Alternative/Exceptional Flows: Invalid credentials trigger an error message.	

Name: Logout from Hospital Account	**ID: H09**
Stakeholders and goals: Hospitals want to end their active session securely.	
Description: Ends the hospital’s current session and redirects to the login page.	
Actors: Hospital Administrator	
Trigger: Hospital administrator clicks “Logout.”	
Normal Flow: **1.** Hospital administrator clicks logout. 2. The system ends the session and clears tokens. 3. Redirects to the login screen.	
Sub-Flows: Session termination.	
Alternative/Exceptional Flows: None.	

Name: Reset Hospital Password	ID: H10
Stakeholders and goals: Hospitals want to recover access if password is forgotten.	
Description: Allows hospital administrators to reset password through email verification.	
Actors: Hospital Administrator	
Trigger: Hospital administrator clicks “Forgot Password.”	
Normal Flow: 1. The hospital enters a registered email. 2. The system checks that the entered email is tied to an existing account. 3. The system sends a reset link. 4. The hospital administrator clicks a link and enters a new password. 5. The hospital administrator re-enters the password to confirm. 6. System confirms reset.	
Sub-Flows: ● Email verification. ● Validate password - Check that new password meets system requirements	
Alternative/Exceptional Flows: ● If the email is not found, show “No account associated.” ● If the password and confirm password do not match, display a message to inform users about it.	

Name: Categorize Disease Genes by Type	ID: H11
Stakeholders and goals: Hospitals want to organize gene entries by disease categories.	
Description: Enables hospital staff to group genes by disease type (e.g., cardiovascular, cancer, neurological).	
Actors: Hospital Administrator	
Trigger: Hospital administrator accesses “Gene Categories.”	
Normal Flow: 1. The system displays a list of available categories.	

2. Admin assigns or creates new categories. 3. The system saves category mappings.
Sub-Flows: Category management.
Alternative/Exceptional Flows: If category name already exists, prompt "Duplicate category."

Name: View Organization Details	**ID: H12**
Stakeholders and goals: Hospitals want to view their organization account's registered information.	
Description: Allow hospital administrators to view the details of their hospital's account so that they can ensure that the information is correct.	
Actors: Hospital Administrator	
Trigger: The hospital administrator clicks "My Account".	
Normal Flow: 1. The hospital administrator logs into the system. 2. The hospital administrator navigates to the organization settings or profile section. 3. The system retrieves the hospital's registered details from the database. 4. The system displays all relevant organization details. 5. The hospital administrator reviews the displayed information.	
Sub-Flows: None	
Alternative/Exceptional Flows: If the details cannot be retrieved by the system due to some error (e.g. network error, database error), display error message.	

Name: Update Organization's Account Information	**ID: H13**
Stakeholders and goals: Hospital wants to make changes to the information listed on their organization's account.	
Description: Allow hospital administrators want to update or correct their organization's registered details to ensure that all records remain accurate and current within the system.	

Actors: Hospital Administrator
Trigger: The hospital's administrator clicks "Edit Account" on their account's page
Normal Flow: 1. The hospital administrator goes to their account page which displays their account details. 2. The hospital administrator clicks on the "Edit Account" option. 3. The system displays all the fields of the current account details. 4. The hospital administrators edit the details in one or more fields. 5. The hospital administrator clicks "Save" once they are done updating the details. 6. The system verifies that the updated information is valid. If it is valid, the system proceeds to save the updated information.
Sub-Flows: Deletion Confirmation
Alternative/Exceptional Flows: ● Upon clicking "Save", if the system detects that the updated information in one or more fields is invalid, an error message is displayed with information on which field is invalid. ● If database update fails, the system displays an error message, "Unable to update information at the moment. Please try again later."

Name: Delete Organization Account	**ID: H14**
Stakeholders and goals: Hospital wants to permanently delete their organization's account from the platform when they no longer wish to provide PSI-based services or if the organization has closed, ensuring that all associated data is securely removed.	
Description: Allow hospital administrators to perform deletion of their organization's account from the system.	
Actors: Hospital Administrator	
Trigger: The hospital administrator selects the "Delete Account" option from the organization settings.	
Normal Flow: 1. The hospital administrator navigates to the organization account settings page. 2. The system displays an option to delete the organization's account.	

3. The hospital administrator clicks “Delete Account.”
4. The system prompts for confirmation, “Are you sure you want to delete this account? This action cannot be undone.”
5. The hospital administrator confirms the deletion request.
6. The system deletes all related data, logs the action, and terminates the organization’s access.
7. The system displays a confirmation message and logs the user out.

Sub-Flows: None

Alternative/Exceptional Flows:

- If the administrator cancels at the confirmation step, the system aborts the deletion process.
- If the deletion process fails, the system aborts the deletion process and displays an error message, “Unable to delete account at this time. Please try again later or contact an administrator.”

Name: Create new disease categories in database	**ID: H15**

Stakeholders and goals: Hospital wants to organize and manage newly discovered diseases effectively by creating new disease categories in the system database.

Description: Allows Hospital Administrators to create new disease categories in the database to classify new disease-gene associations, ensuring that patient and research data remain well-organized and searchable.

Actors: Hospital Administrator

Trigger: Hospital Administrator clicks on the “Add New Disease Category” button in the Disease Management section of the hospital system.

Normal Flow:

1. The hospital administrator navigates to the “Disease Categories” management section.
2. The hospital administrator selects the option to “Add New Category.”
3. The system prompts the hospital administrator to enter the category name, description, and related attributes.
4. The hospital administrator fills in the required details and submits the form.

5. The system validates the input and saves the new disease category into the database.

6. The system confirms successful creation with a message.

Sub-Flows: None

Alternative/Exceptional Flows:
- If mandatory fields are left blank, the system displays an error and prompts for correction.
- If a duplicate category name already exists, the system notifies the administrator and prevents duplication.
- If the database connection fails, the system alerts the administrator and logs the issue for technical review.

Name: View all disease categories in database	**ID: H16**

Stakeholders and goals: Hospital wants to view all disease categories in the database to ensure data accuracy, monitor stored gene records, and support ongoing research updates.

Description: Allows the hospital administrator to view all disease categories stored in its database to understand how gene information is organized.

Actors: Hospital Administrator

Trigger: The hospital administrator selects “View All Disease Categories” from the system menu.

Normal Flow:
1. The hospital administrator navigates to the “Disease Categories” section.

2. The system retrieves all disease category records from the database.

3. The system displays the list of disease categories, including names and brief descriptions.

4. The hospital administrator reviews the categories and may scroll or filter as needed.

Sub-Flows: None

Alternative/Exceptional Flows:
- If no disease categories exist, the system displays a message: “No disease categories found.”
- If a database connection error occurs, the system displays an error message and logs the issue.

Name: Update disease category information	ID: H17
Stakeholders and goals: Hospital wants to update disease category names or descriptions to ensure that all classifications remain consistent with current medical standards.	
Description: Allows the hospital administrator to modify existing disease category names or descriptions in the database to reflect updated information or medical terminology.	
Actors: Hospital Administrator	
Trigger: The hospital administrator selects a specific disease category and chooses the option to update its details.	
Normal Flow: 1. The hospital administrator logs into the system. 2. The hospital administrator navigates to the “Disease Categories” section. 3. The hospital administrator clicks “Edit Category” for a specific disease category to update. 4. The system displays the current information for that category. 5. The hospital administrator edits the desired fields. 6. The hospital administrator clicks on “Save” to confirm their changes. 7. The system verifies that the updates are valid. If they are, it updates the database and displays a success message.	
Sub-Flows: None	
Alternative/Exceptional Flows: ● If the hospital administrator leaves required fields blank, the system prompts them to fill in the missing details. ● If the update fails due to a system or database error, an error message is displayed, and no changes are saved.	

Name: Search for a disease category	ID: H18
Stakeholders and goals: Hospital wants to search for specific disease categories to quickly find and manage relevant entries in large databases.	
Description: Allows the hospital administrator to search for specific disease categories in the database using keywords, improving efficiency in locating and	

managing medical data.
Actors: Hospital Administrator
Trigger: The hospital administrator clicks on the “Search Disease Categories” option in the Disease Management section.
Normal Flow: 1. The hospital administrator navigates to the Disease Management section. 2. The hospital administrator clicks on Search Disease Categories. 3. The system displays a search bar or filter panel. 4. The hospital administrator enters a keyword or search criteria. 5. The system retrieves and displays matching disease categories with their details. 6. The hospital administrator reviews or selects a category for further actions if needed.
Sub-Flows: Search and filter functions.
Alternative/Exceptional Flows: ● If no results match the search, the system displays a message: “No matching disease categories found.” ● If a system or database error occurs, an error message is displayed and logged.

Name: Delete unused disease categories	**ID: H19**
Stakeholders and goals: Hospital wants to	
Description: Allows the hospital administrator to remove unused or irrelevant disease categories from the database to maintain accurate and relevant records.	
Actors: Hospital Administrator	
Trigger: The hospital administrator clicks on the “Delete Disease Category” option in the Disease Management section.	
Normal Flow: 1. The hospital administrator logs into the system. 2. The hospital administrator navigates to the Disease Management section. 3. The hospital administrator selects the disease category to be deleted.	

4. The hospital administrator clicks on the Delete Disease Category option.
5. The system prompts for confirmation before deletion.
6. The hospital administrator confirms the deletion.
7. The system removes the selected disease category from the database.
8. The system displays a success message confirming the deletion.

Sub-Flows: None

Alternative/Exceptional Flows:
- If the administrator cancels the confirmation, the deletion is aborted.
- If the disease category is linked to other records (e.g. gene data), the system prevents deletion and displays an error message.
- If a database or system error occurs, an appropriate error message is displayed and logged.

Name: Search for a gene	**ID: H20**

Stakeholders and goals: Hospital wants to search for specific gene records in its database to quickly locate and verify information for updates or analysis.

Description: Allows the hospital administrator to search for specific genes using keywords, gene IDs, or related disease names, enabling faster access to gene data for verification or updates.

Actors: Hospital Administrator

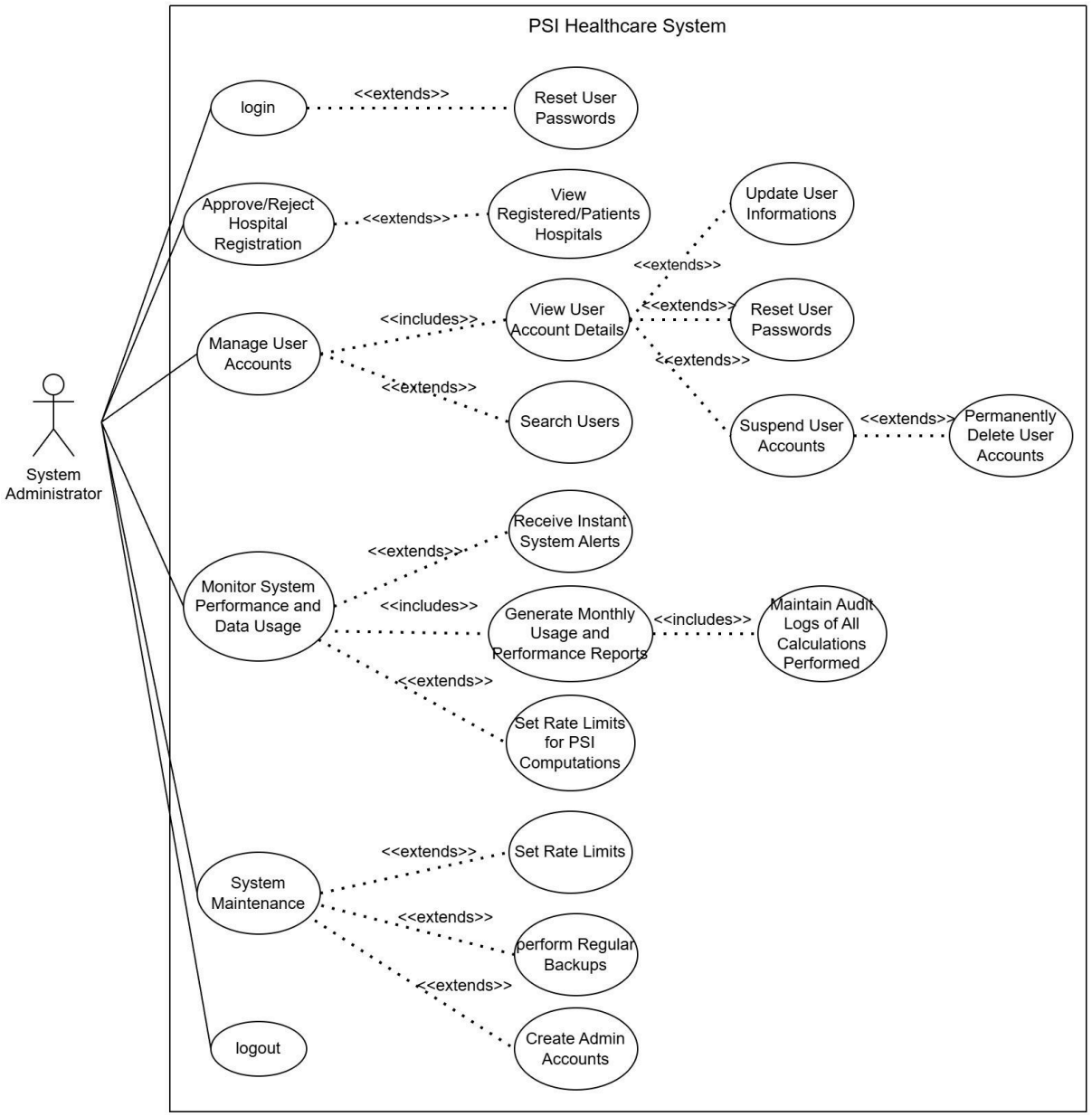
Trigger: The hospital administrator clicks the “Search Genes ” option.

Normal Flow:
1. The hospital administrator logs into the system.
2. The hospital administrator navigates to the Gene Management section.
3. The hospital administrator clicks on Search Genes.
4. The system displays a search bar and optional filter options.
5. The hospital administrator enters the gene name, ID, or keyword.
6. The system queries the database for matching gene records.
7. The system displays a list of results with key details (e.g., gene name, category, description).

8. The hospital administrator selects a gene record to view details or proceed with updates.
Sub-Flows: Search and filter functions.
Alternative/Exceptional Flows: ● If no matching gene is found, the system displays “No matching gene records found.” ● If a database or system error occurs, the system displays an error message and logs the issue.

8.1.3 System Administrator

8.1.3.1 Use Case Diagram


PSI Healthcare System
System Administrator
login
Reset User Passwords
Approve/Reject Hospital Registration
View Registered/Patients Hospitals
Update User Informations
View User Account Details
Reset User Passwords
Manage User Accounts
Search Users
Suspend User Accounts
Permanently Delete User Accounts
Receive Instant System Alerts
Monitor System Performance and Data Usage
Generate Monthly Usage and Performance Reports
Maintain Audit Logs of All Calculations Performed
Set Rate Limits for PSI Computations
Set Rate Limits
System Maintenance
perform Regular Backups
Create Admin Accounts
logout
<<extends>>
<<includes>>

8.1.3.2 User Stories

No	System Admin User Stories
1	As a system administrator, I want to approve or reject hospital registration requests, so that I can ensure that only legitimate healthcare providers access the system.
2	As a system administrator, I want to maintain audit logs of all calculations performed, so that patients receive accurate risk calculations.
3	As a system administrator, I want to login to my admin account, so that I can securely access administrative functions.
4	As a system administrator, I want to logout of my admin account, so that I can maintain the security and privacy when leaving my workstation.
5	As a system administrator, I want to search for registered patients and hospitals, so that I can easily access the details of all users on the platform.
6	As a system administrator, I want to be able to reset passwords for users who are locked out, so that I can help users regain access when needed.
7	As a system administrator, I want to monitor system performance and data usage, so that I can ensure the PSI platform runs smoothly and efficiently without downtime.
8	As a system administrator, I want to perform regular backups of system data, so that information can be recovered in case of data loss or corruption.
9	As a system administrator, I want to receive instant alerts if the PSI system goes down, so that I can quickly take action to restore services.
10	As a system administrator, I want to generate monthly usage and performance reports, so that I can track system health and prepare for audits.
11	As a system administrator, I want to set rate limits on how many PSI computations a patient or hospital can perform per day, so that I can prevent system abuse and ensure fair resource allocations across all users.
12	As a system administrator, I want to view detailed information about any user account (patient, hospital, researcher), so that I can investigate issues and provide support when needed.
13	As a system administrator, I want to update user account information when authorized to do so, so that I can correct errors or assist users with account issues.
14	As a system administrator, I want to suspend user accounts that violate terms of service, so that I can maintain platform integrity and protect other users.
15	As a system administrator, I want to permanently delete user accounts upon request or after deactivation period, so that I can comply with data protection

	regulations and user rights.
16	As a System Admin,I want to reset my password if I forget it,so that I can regain access to my account without losing my data.
17	As a System Admin, I want to view my account details, so that I can verify my personal information is accurate and up to date.
18	As a System Admin, I want to update my account information (email, contact details, password), so that I can keep my profile current and maintain secure access to the system.
19	As a system administrator, I want to create additional system administrator and system security user accounts, so that I can onboard authorized personnel to help manage and secure the PSI platform as the team grows

8.1.3.3 Use Case Description

Name: Approve or Reject Hospital Registration Requests	**ID: A01**
Stakeholders and goals: System administrators want to ensure that only verified hospitals can access the PSI platform.	
Description: Enables administrators to review and approve or reject new hospital registration applications.	
Actors: System Administrator	
Trigger: A new hospital registration request is submitted.	
Normal Flow: 1. Administrator logs into the system. 2. Views list of pending hospital registration requests. 3. Reviews hospital details and supporting documents. 4. Approves or rejects each request. 5. The system notifies the hospital of the decision.	
Sub-Flows: Hospital verification process.	
Alternative/Exceptional Flows: If hospital data is incomplete or invalid, the system requests resubmission.	

Name: Maintain Audit Logs of Calculations	**ID: A02**

Stakeholders and goals: Administrators want to ensure transparency and traceability of PSI computations.
Description: Allows administrators to view, manage, and store detailed logs of all PSI calculations performed.
Actors: System Administrator
Trigger: System automatically logs computation activities or admin manually requests logs.
Normal Flow: 1. Administrator accesses the “Audit Logs” page. 2. The system retrieves logs of all PSI activities. 3. Administrator filters, views, or exports logs.
Sub-Flows: Log search and export.
Alternative/Exceptional Flows: If logs are corrupted or missing, the system displays an error message.

Name: Login to Admin Account	**ID: A03**
Stakeholders and goals: Administrators need secure access to the management dashboard.	
Description: Enables admin to authenticate and access the system.	
Actors: System Administrator	
Trigger: Administrator selects the “Login” option.	
Normal Flow: 1. Admin enters username and password. 2. System validates credentials. 3. The system establishes a secure session for the user. 4. Admin is redirected to the dashboard.	
Sub-Flows: Authentication and session creation.	
Alternative/Exceptional Flows: Invalid credentials prompt an error message.	

Name: Logout of Admin Account	ID: A04
Stakeholders and goals: Administrators want to end their session securely.	
Description: Ends the admin's current session and returns to the login page.	
Actors: System Administrator	
Trigger: Admin clicks "Logout."	
Normal Flow: 1. Admin selects the logout option. 2. System terminates session and clears cache. 3. Redirects to the login page.	
Sub-Flows: Session invalidation.	
Alternative/Exceptional Flows: None.	

Name: View Registered Patients and Hospitals	ID: A05
Stakeholders and goals: Admin wants an overview of all registered users.	
Description: Displays a list of all registered patients and hospital organizations.	
Actors: System Administrator	
Trigger: Admin accesses the "User Management" section.	
Normal Flow: 1. The system retrieves all user records. 2. Admin can view, filter, or sort the list.	
Sub-Flows: Search and filter options.	
Alternative/Exceptional Flows: If no records are found, the system displays "No users available."	

Name: Reset User Passwords	ID: A06
Stakeholders and goals: Admin helps users regain account access.	
Description: Allows the administrator to reset passwords for patients or hospitals who are locked out.	

Actors: System Administrator
Trigger: Admin receives password reset request.
Normal Flow: 1. Admin selects the affected user. 2. Click “Reset Password.” 3. The system generates and sends a reset link or temporary password.
Sub-Flows: Notification and confirmation.
Alternative/Exceptional Flows: If email fails to send, the system displays an error message.

Name: Monitor System Performance and Data Usage	**ID: A07**
Stakeholders and goals:	
Description: Admin wants to ensure the system runs efficiently.	
Actors: System Administrator	
Trigger: Allows monitoring of CPU load, storage, and PSI task frequency.	
Normal Flow: 1. Admin views system metrics and usage graphs. 2. Identifies abnormal activity or performance issues.	
Sub-Flows: Data analytics retrieval.	
Alternative/Exceptional Flows: If metrics unavailable, display “No data currently available.”	

Name: Perform Regular Backups of System Data	**ID: A08**
Stakeholders and goals: Admin wants to prevent data loss.	
Description: Enables admin to back up user data, PSI logs, and configurations.	
Actors: System Administrator	
Trigger: Backup schedule reached or manually initiated.	

Normal Flow: 1. Admin selects a backup option. 2. The system compresses and stores data backup securely. 3. Confirmation is displayed.
Sub-Flows: Backup verification.
Alternative/Exceptional Flows: If backup fails, system logs the error and alerts admin.

Name: Receive Instant System Alerts	**ID: A09**
Stakeholders and goals: Admin wants immediate notification of system failures or security incidents.	
Description: System sends automated alerts to the administrator during anomalies or downtime.	
Actors: System Administrator	
Trigger: System detects performance issues or unauthorized access attempts.	
Normal Flow: 1. The system generates alerts. 2. Notification is sent via email or dashboard message. 3. Admin reviews alerts and takes corrective action.	
Sub-Flows: Alert acknowledgement.	
Alternative/Exceptional Flows: If notification system fails, alerts are logged for later viewing.	

Name: Generate Monthly Usage and Performance Reports	**ID: A10**
Stakeholders and goals: Admin wants to track system usage and prepare reports for audits.	
Description: Enables generating monthly PSI usage statistics and system performance summaries.	
Actors: System Administrator	
Trigger: Admin selects “Generate Monthly Report.”	

Normal Flow: 1. The system gathers logs and usage data. 2. Generates formatted reports. 3. Admin views or exports report.
Sub-Flows: Report generation and export.
Alternative/Exceptional Flows: If report generation fails, display “Error retrieving data.”

Name: Set Rate Limits for PSI Computations	**ID: A11**
Stakeholders and goals: Admin wants to prevent system abuse and manage load.	
Description: Allows admin to define daily or per-user limits on PSI computations.	
Actors: System Administrator	
Trigger: Admin navigates to “Rate Limit Settings.”	
Normal Flow: 1. Admin defines new rate limits for patients and hospitals. 2. The system applies and enforces limits automatically. 3. Confirmation displayed.	
Sub-Flows: Rule validation.	
Alternative/Exceptional Flows: If invalid limit entered, system prompts for correction.	

Name: View User Account Details	**ID: A12**
Stakeholders and goals: Admin wants to access detailed information about any registered user.	
Description: Allows admins to view detailed information about a specific user account within the platform.	
Actors: System Administrator	
Trigger: The system administrator selects a user from the list of registered accounts or searches for a user by ID, email, or organization name.	

Normal Flow:

1. The administrator navigates to the “User Management” section.
2. The administrator searches for or selects a user account.
3. The system retrieves the selected user’s details from the database.
4. The system displays all relevant information.
5. The administrator reviews the information for verification or issue resolution.

Sub-Flows: The system allows filtering by user type (e.g. Patient, Hospital)

Alternative/Exceptional Flows:

- If the search query returns no results, the system displays “No user found.”
- If the system cannot retrieve user details (e.g., database error), an error message appears: “Unable to load user details. Please try again later.”

Name: Update User Account Information	**ID: A13**

Stakeholders and goals: Admin wants to update or correct user account information to resolve issues, correct data entry errors, or assist users who are unable to make changes themselves.

Description: Allows admin to modify user account details when authorized to do so. It ensures that incorrect or outdated user information can be rectified efficiently while maintaining data integrity, audit logging, and compliance with access control policies.

Actors: System Administrator

Trigger: The admin selects a specific user account and clicks on “Edit Account Details”

Normal Flow:

1. The administrator navigates to the User Management section.
2. The administrator searches for and selects a specific user account.
3. The system displays the current user details.
4. The administrator edits one or more fields (e.g., email, contact number, account role, organization affiliation).
5. The administrator clicks on “Save”.

6. The system validates the updated information for correct format and completeness.

7. If the updated information is valid, the system saves the changes and displays a confirmation message.

Sub-Flows:

Alternative/Exceptional Flows:

- If input validation fails (e.g., invalid email format, missing required fields), the system highlights errors and prevents submission.
- If the database update fails, display: “Unable to update user information at this time. Please try again later.”

Name: Suspend User Account	**ID: A14**

Stakeholders and goals: Admin wants to temporarily suspend user accounts that violate the platform’s terms of service or exhibit suspicious activity, so that they can protect other users and maintain the integrity of the PSI system.

Description: Allows the admin to suspend a user’s account, restricting the user’s access to the platform without permanently deleting their data.

Actors: System Administrator

Trigger: The system administrator selects a specific user account from the User Management dashboard and clicks the “Suspend Account” option.

Normal Flow:

1. The administrator navigates to the User Management section.

2. The administrator searches for and selects the target user account.

3. The system displays the user’s profile and current account status.

4. The administrator clicks “Suspend Account.”

5. The system prompts for confirmation and an optional reason for suspension.

6. The administrator confirms the action.

7. The system updates the account status to “Suspended.”

8. The system notifies the user by email of the suspension and reason provided.

9. The suspension event is recorded in the system audit log.

Sub-Flows: The system automatically revokes the user’s active sessions and API

tokens.
Alternative/Exceptional Flows: ● If the administrator cancels during the confirmation step, the suspension process is aborted. ● If the database update fails, display: “Unable to suspend account. Please try again later.”

Name: Permanently Delete User Account	**ID: A15**
Stakeholders and goals: Admin wants to permanently delete user accounts that have been deactivated, requested removal, or are no longer needed.	
Description: Allows admin to permanently remove a user account and all associated data from the system.	
Actors: System Administrator	
Trigger: The admin selects a user account marked for deletion or manually initiates a permanent delete action by clicking “Delete Account Permanently” from the User Management dashboard.	
Normal Flow: 1. The administrator navigates to the User Management section. 2. The administrator searches for and selects the user account to be deleted. 3. The system displays the account details and a confirmation warning. 4. The administrator reviews the data and clicks “Delete Account Permanently” 5. The system prompts for confirmation with the message, “Are you sure you want to delete this account permanently? This action cannot be undone.” 6. The administrator confirms deletion. 7. The system removes the user account and all associated data from active storage. 8. The system displays a confirmation message.	
Sub-Flows: ● The system performs dependency checks to ensure no active PSI computations, hospital requests, or linked research data remain. ● If dependencies exist, the system prompts the administrator to transfer or archive related data before deletion.	
Alternative/Exceptional Flows: ● If the administrator cancels during confirmation, the deletion process is	

aborted.
- If the system encounters a database or storage error, display: “Deletion failed. Please try again later.”

Name: Reset System Administrator Password	ID: A16

Stakeholders and goals: Admin wants to securely reset their password when they forget it, so that they can regain access to their administrative account without compromising platform security.

Description: Enables an admin to recover account access through a secure password reset process. It ensures that only authorized administrators can reset passwords, using multi-factor authentication or secure verification links to maintain system integrity.

Actors: System Administrator

Trigger: The administrator clicks the “Forgot Password” option on the login page or initiates a password reset from their account settings.

Normal Flow:

1. The admin clicks “Forgot Password” from the login page or “Reset Password” from account settings.
2. The system prompts the administrator to enter their registered email address.
3. The system verifies that the email address belongs to a valid admin account.
4. The system generates a secure, time-limited reset token and sends a password reset link to the email.
5. Admin clicks the link and is redirected to the password reset page.
6. Admin enters a new password twice for confirmation.
7. Admin clicks “Reset Password”
8. The system validates the password (e.g. minimum length, character complexity).
9. If the password is valid, the system updates the password in the database and invalidates the old one.
10. The system displays a confirmation message indicating successful password reset.
11. The admin can now log in with the new credentials.

Sub-Flows:

- The reset link expires after a set period.
- The system sends a follow-up email notifying the admin that their password has been changed.

Alternative/Exceptional Flows:

- If the entered email is not found, display: “No account associated with this email.”
- If the reset token has expired or been used already, display: “Invalid or expired link. Please request a new reset.”
- If password validation fails, display a message informing the admin about the password requirements.
- If the database update fails, display an error message, “Unable to reset password. Please try again later.”

Name: View System Administrator Account Details	**ID: A17**

Stakeholders and goals: Admin wants to view their own account details, such as name, email, role, and contact information, so that they can verify that their personal information

Description: Allow admin to view their profile information within the admin dashboard. It ensures transparency and enables administrators to confirm that their account details are correct

Actors: System Administrator

Trigger: The system administrator selects the “My Account” option from the admin dashboard navigation menu.

Normal Flow:

1. The system administrator logs into the admin dashboard.
2. The administrator clicks the “My Account” or “Profile” tab.
3. The system retrieves the administrator’s stored account details from the database.
4. The system displays relevant information
5. The administrator reviews their account details.

Sub-Flows:

Alternative/Exceptional Flows: If the system cannot retrieve the account details (e.g. database error), display: “Unable to load account details. Please try again later.”

Name: Update System Administrator Account Information	ID: A18
Stakeholders and goals: Admin wants to update their own account information, such as email, contact details, or password, so that they can keep their profile current and maintain secure access to the system.	
Description: Allow the system administrator to edit and update their personal account details from within the admin dashboard to ensure that their contact and authentication information remain accurate.	
Actors: System Administrator	
Trigger: The system administrator selects the “Edit Account” option from the profile page.	
Normal Flow: 1. The administrator navigates to the “My Account” section. 2. The system displays the current account information. 3. The administrator edits one or more fields. 4. The system validates all input fields for correctness and format. 5. The administrator confirms and submits the changes. 6. The system updates the account information in the database. 7. The system displays a confirmation message indicating successful update.	
Sub-Flows: None	
Alternative/Exceptional Flows: ● If input validation fails (e.g. invalid email format, weak password), the system displays an error message and prevents submission. ● If the database update fails, display: “Unable to update account information. Please try again later.” ● If the session expires before submission, the system prompts for re-login before proceeding.	

Name: Create system administrator and security user accounts	ID: A19
Stakeholders and goals: Admin wants to create additional administrator and system security accounts to onboard authorized personnel for platform management and security operations.	
Description: Enables the system administrator to register new system administrator and system security user accounts in the PSI platform, granting them appropriate roles and access permissions.	

Actors: System Administrator

Trigger: The system administrator clicks on the “Create New Admin/Security Account” option in the User Management section.

Normal Flow:

1. The administrator navigates to the User Management section.
2. The administrator clicks on Create New Admin/Security Account.
3. The system displays a registration form for account creation.
4. The administrator fills in details such as name, email, role (Admin/Security), and temporary password.
5. The administrator submits the form.
6. The system validates the inputs and creates the new user account.
7. The system sends a confirmation email to the new user with login credentials and password reset instructions.
8. The system displays a message confirming successful account creation.

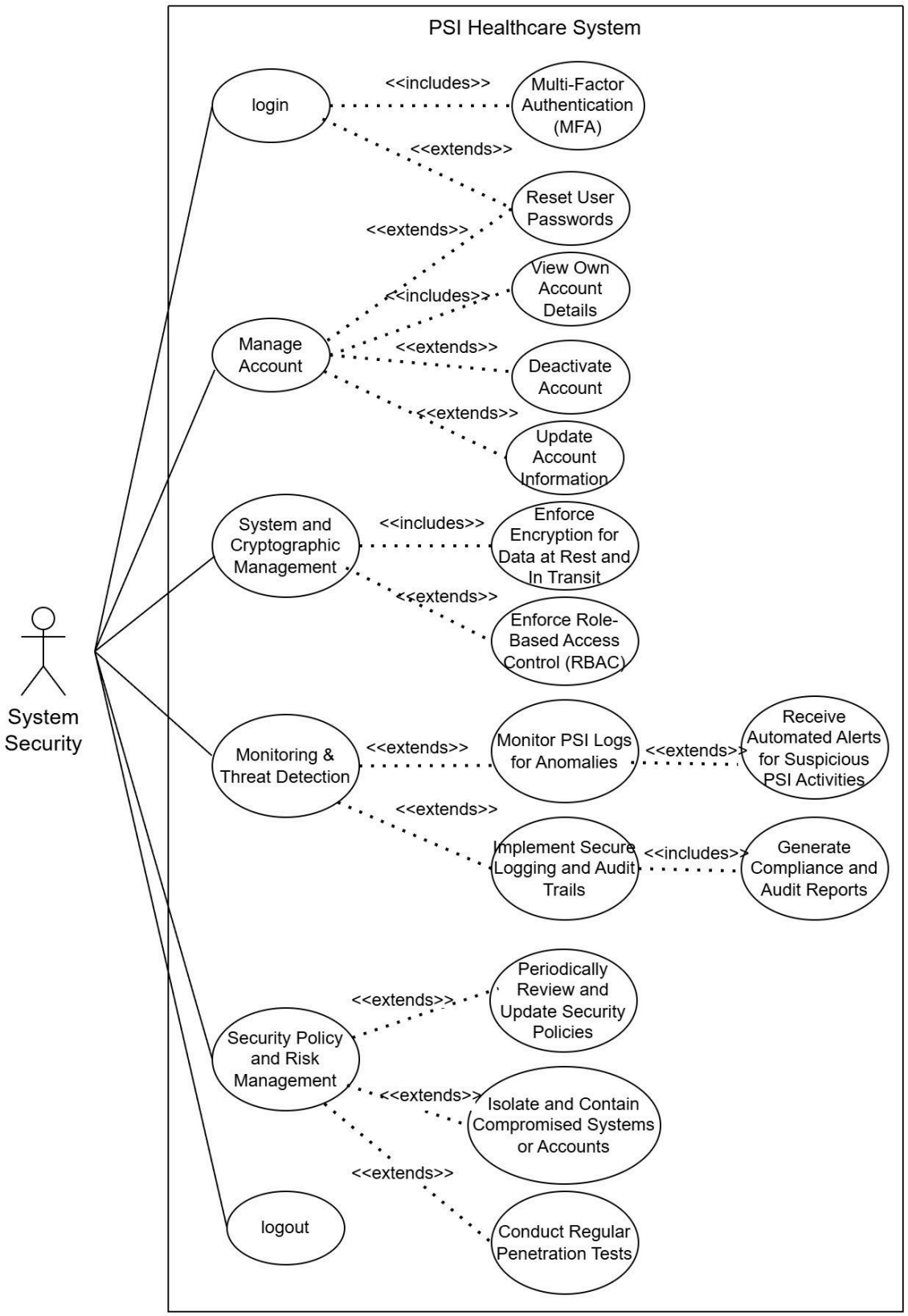
Sub-Flows: Role and Permission Assignment

Alternative/Exceptional Flows:

- If any required field is missing, the system prompts the administrator to complete it.
- If the entered email already exists, the system displays a “User already registered” message.
- If a system or database error occurs, the system displays an error message and logs the issue for review.

8.1.4 System Security

8.1.4.1 Use Case Diagram



8.1.4.2 User Stories

No.	System Security User Stories
1	As a system security user, I want to manage and rotate cryptographic keys used in PSI, so that the data exchanges between healthcare providers remain secure.
2	As a system security user, I want to enforce encryption of all data at rest and in transit in the PSI system,so that sensitive healthcare data remains protected against unauthorized access.
3	As a system security user, I want to enforce role-based access control for PSI system users, so that only authorized staff can access or configure sensitive components.
4	As a system security user, I want to monitor PSI logs for anomalies, so that I can detect potential breaches in the intersection process.
5	As a system security user, I want to receive automated alerts for suspicious PSI activities, so that I can respond quickly to potential security breaches.
6	As a system security user, I want to generate compliance and audit reports of PSI transactions, so that I can demonstrate adherence to privacy regulations.
7	As a system security user, I want to implement secure logging and audit trails for all PSI operations, so that I can trace back actions in case of security incidents.
8	As a system security user, I want to periodically review and update the system's security policies, so that the PSI platform continues to comply with evolving privacy laws and standards.
9	As a system security user, I want to conduct regular penetration tests on the PSI system, so that I can identify and fix vulnerabilities before attackers exploit them.
10	As a system security user, I want to isolate and contain compromised accounts or systems automatically, so that I can minimize damage and prevent the spread of a security breach.
11	As a system security user, I want to implement multi-factor authentication (MFA) for all hospital administrator accounts, so that disease gene databases are protected from unauthorized access even if passwords are compromised.
12	As a system security, I want to login to my account, so that I can securely access administrative security functions.
13	As a system security, I want to logout of my admin account, so that I can maintain the security and privacy when leaving my workstation.
14	As a System Security,I want to reset my password if I forget it,so that I can regain access to my account without losing my data.
15	As a System Security, I want to view my account details, so that I can verify my personal information is accurate and up to date.
16	As a System Security, I want to update my account information (email, contact details, password), so that I can keep my profile current and maintain secure access to the system.

8.1.4.3 Use Case Description

Name: Manage and Rotate Cryptographic Keys	ID: S01
Stakeholders and goals: Security users want to maintain strong encryption to protect PSI communications.	
Description: Allows system security users to manage and periodically rotate cryptographic keys used in PSI computations.	
Actors: System Security User	
Trigger: Key rotation schedule reached or manual update initiated.	
Normal Flow: 1. Security user logs into security console. 2. Navigates to the key management section. 3. Generates or uploads new keys. 4. The system distributes new keys securely to authorized modules.	
Sub-Flows: Key validation and distribution.	
Alternative/Exceptional Flows: If key validation fails, the system reverts to the previous valid key and notifies admin.	

Name:Enforce Data Encryption at Rest and In Transit	ID: S02
Stakeholders and goals: Security users want all sensitive data to remain encrypted throughout its lifecycle.	
Description: Ensures encryption of patient and hospital data both in storage and during transmission.	
Actors: System Security User	
Trigger: Security configuration setup or audit process.	
Normal Flow: 1. Security user verifies current encryption settings. 2. Enables encryption protocols (e.g., AES, TLS). 3. System confirms data encryption status.	
Sub-Flows: Encryption policy update.	

Alternative/Exceptional Flows: If the encryption library fails to load, the system disables data transfers and alerts the admin.

Name: Enforce Role-Based Access Control (RBAC)	**ID: S03**
Stakeholders and goals: Security users want only authorized personnel to access sensitive modules.	
Description: Defines and applies access control policies for different user roles (patient, hospital, admin).	
Actors: System Security User	
Trigger: New user roles are created or permissions updated.	
Normal Flow: 1. The security user opens the access control settings. 2. Assigns roles and defines permissions. 3. The system enforces restrictions automatically.	
Sub-Flows: Role and permission mapping.	
Alternative/Exceptional Flows: If conflicting permissions are detected, the system prevents update and logs warning.	

Name: Monitor PSI Logs for Anomalies	**ID: S04**
Stakeholders and goals: Security users want to detect irregular activities in PSI computations.	
Description: Allows continuous monitoring of PSI transaction logs for suspicious patterns or unauthorized access.	
Actors: System Security User	
Trigger: Periodic log review or alert from monitoring tool.	
Normal Flow: 1. Security user accesses log monitoring dashboard. 2. Reviews PSI computation logs. 3. Flags anomalies for further investigation.	
Sub-Flows: Automated anomaly detection.	

Alternative/Exceptional Flows: If logs are unavailable, display “No recent activity found.”

Name: Receive Automated Alerts for Suspicious Activities	**ID: S05**
Stakeholders and goals: Security users want immediate alerts for potential security breaches.	
Description: System generates and sends real-time notifications when suspicious or unusual PSI behavior is detected.	
Actors: System Security User	
Trigger: Detected anomaly or intrusion event.	
Normal Flow: 1. The system identifies irregular PSI activity. 2. Send an alert to the security dashboard or email. 3. Security user reviews and investigates.	
Sub-Flows: Alert prioritization and response tracking.	
Alternative/Exceptional Flows: If alert delivery fails, alert is stored in system logs for manual review.	

Name: Generate Compliance and Audit Reports	**ID: S06**
Stakeholders and goals: Security users want to ensure the PSI platform meets data protection regulations.	
Description: Enables generation of detailed compliance and audit reports for privacy audits.	
Actors: System Security User	
Trigger: Scheduled compliance review or audit request.	
Normal Flow: 1. The security user opens the “Compliance Reports” tab. 2. Selects report type and time range. 3. The system compiles and displays reports. 4. User exports report as PDF or CSV.	

Sub-Flows: Data retrieval and formatting.
Alternative/Exceptional Flows: If data is incomplete, the system indicates “Partial report generated.”

Name: Implement Secure Logging and Audit Trails	**ID: S07**
Stakeholders and goals: Security users need to ensure accountability in PSI operations.	
Description: Configures the system to maintain tamper-proof logs for all critical security events.	
Actors: System Security User	
Trigger: Log configuration setup or update.	
Normal Flow: 1. The security user defines which events to log. 2. The system starts recording actions in secure logs. 3. Logs are timestamped and encrypted.	
Sub-Flows: Log rotation and archival.	
Alternative/Exceptional Flows: If log storage is full, the system alerts the admin to expand capacity.	

Name: Review and Update Security Policies	**ID: S08**
Stakeholders and goals: Security users want to keep the system compliant with evolving laws and standards.	
Description: Allows periodic review and updating of system-wide security policies.	
Actors: System Security User	
Trigger: Scheduled policy audit or regulatory update.	
Normal Flow: 1. Security users review existing policies. 2. Edits or adds new security requirements. 3. The system validates and applies updated policies.	

Sub-Flows: Policy versioning.
Alternative/Exceptional Flows: If policy conflicts are detected, the system requests manual confirmation before applying.

Name: Conduct Regular Penetration Tests	**ID: S09**
Stakeholders and goals: Security users want to identify vulnerabilities before attackers exploit them.	
Description: Simulates attacks to test the PSI system's security defenses.	
Actors: System Security User	
Trigger: Scheduled penetration test or after major system update.	
Normal Flow: 1. Security user initiates test session. 2. The system runs authorized penetration test scripts. 3. Vulnerabilities are logged and reported.	
Sub-Flows: Vulnerability scoring.	
Alternative/Exceptional Flows: If a test fails or impacts the live system, it is halted and rolled back.	

Name: Isolate and Contain Compromised Accounts or Systems	**ID: S10**
Stakeholders and goals: Security users want to limit damage during a breach.	
Description: Automatically isolates suspicious user accounts or systems to prevent spread of attack.	
Actors: System Security User	
Trigger: Intrusion or compromise detected.	
Normal Flow: 1. The system identifies compromised users or nodes. 2. Automatically restricts its access. 3. Security user reviews and reactivates after verification.	
Sub-Flows: Isolation and restoration.	

Alternative/Exceptional Flows: If containment fails, escalate to full system lockdown.

Name: Implement Multi-Factor Authentication (MFA) for Hospital Admins	**ID: S11**
Stakeholders and goals: Security users want stronger authentication for high-privilege accounts.	
Description: Adds MFA to hospital administrator logins to prevent unauthorized access.	
Actors: System Security User	
Trigger: Hospital administrator login or MFA configuration update.	
Normal Flow: 1. Security user enables MFA in settings. 2. Hospital admin enrolls second factor (OTP, authenticator app, etc.). 3. The system enforces MFA on all future logins.	
Sub-Flows: MFA setup and verification.	
Alternative/Exceptional Flows: If MFA devices are unavailable, admin can use backup recovery codes.	

Name: Login to System Security Account	**ID: S12**
Stakeholders and goals: System security users want to log in securely to access administrative security functions, so that they can monitor, configure, and manage the platform's security without unauthorized access.	
Description: Allow a system security user to authenticate and gain access to the security management dashboard using valid credentials. The process ensures secure access control and protects sensitive PSI configuration tools from unauthorized use.	
Actors: System Security User	
Trigger: The system security user navigates to the System Security Login page and enters their credentials.	
Normal Flow: 1. The system security user opens the security login page. 2. The user enters their registered username and password.	

3. The system validates the credentials against stored records.
4. The system establishes a secure session for the user.
5. The user is redirected to the Security Dashboard upon successful login.

Sub-Flows: Authentication process.

Alternative/Exceptional Flows:
- If the entered credentials are invalid, the system displays: “Incorrect email or password.”
- If the account is suspended or deactivated, display: “Your account has been restricted. Contact the system administrator.”

Name: Logout from System Security Account	**ID: S13**

Stakeholders and goals: System security users want to securely log out of their account when they finish their session, so that unauthorized users cannot access sensitive administrative functions.

Description: Allow system security users to safely terminate their current session and exit the platform.

Actors: System Security User

Trigger:.The system security user selects the “Logout” option from the security dashboard or navigation menu.

Normal Flow:
1. The system security user clicks the “Logout” button.
2. The system terminates the active session.
3. The system clears all authentication tokens and temporary cache.
4. The system redirects the user to the login page.
5. The system displays a message confirming successful logout.

Sub-Flows: Session termination

Alternative/Exceptional Flows: None

Name: Reset System Security Account Password	**ID: S14**

Stakeholders and goals: System security users want to securely reset their password when they forget it, so that they can regain access to their account

while maintaining the security of the platform.
Description: Enable system security users to reset their forgotten password through a secure verification process.
Actors: System Security User
Trigger: The system security user selects the “Forgot Password” option on the login page
Normal Flow: 1. The system security user clicks “Forgot Password.” 2. The system prompts for the registered email address. 3. The system verifies that the email belongs to a valid security account. 4. The system generates a secure reset token and sends a password reset link to the user’s email. 5. The user clicks the link and is directed to the reset page. 6. The user enters a new password and confirms it. 7. The system validates the new password (length, complexity, etc.). 8. The system updates the password and invalidates the old one. 9. The system displays a success message confirming the password reset.
Sub-Flows: Email verification and token validation.
Alternative/Exceptional Flows: ● If the email is not associated with any account, display the error message: “Account not found”. ● If the reset link is expired or invalid, display: “This link has expired or is invalid. Please request a new reset link.” ● If password validation fails, display a message informing the admin about the password requirements.

Name: View System Security Account Details	**ID: S15**
Stakeholders and goals: System Security user wants to view their own account details, such as name, email, role, and contact information, so that they can verify that their personal information is correct.	
Description: Allow System Security users to view their account information.	

Actors: System Security User
Trigger: System Security user selects the “My Account” option from the admin dashboard navigation menu.
Normal Flow: 1. The system security user logs into the admin dashboard. 2. The system security user clicks the “My Account” or “Profile” tab. 3. The system retrieves the system security user’s stored account details from the database. 4. The system displays relevant information 5. The system security user reviews their account details.
Sub-Flows: Email verification and token validation.
Alternative/Exceptional Flows: If the system cannot retrieve the account details (e.g. database error), display: “Unable to load account details. Please try again later.”

Name: Update System Security Account Information	**ID: S16**
Stakeholders and goals: System security users want to keep their personal and login details up to date to maintain secure access.	
Description: Allows the system security user to update their account details such as email, contact number, or password to ensure current and secure information.	
Actors: System Security User	
Trigger: The user selects “Edit Profile” or “Update Account Information” from the account settings page.	
Normal Flow: 1. The user enters updated account information. 2. The system validates the new information (e.g. proper email format, strong password). 3. The system saves the new data securely in the database. 4. A confirmation message is displayed to the user.	
Sub-Flows: Email validation and password encryption before storage.	

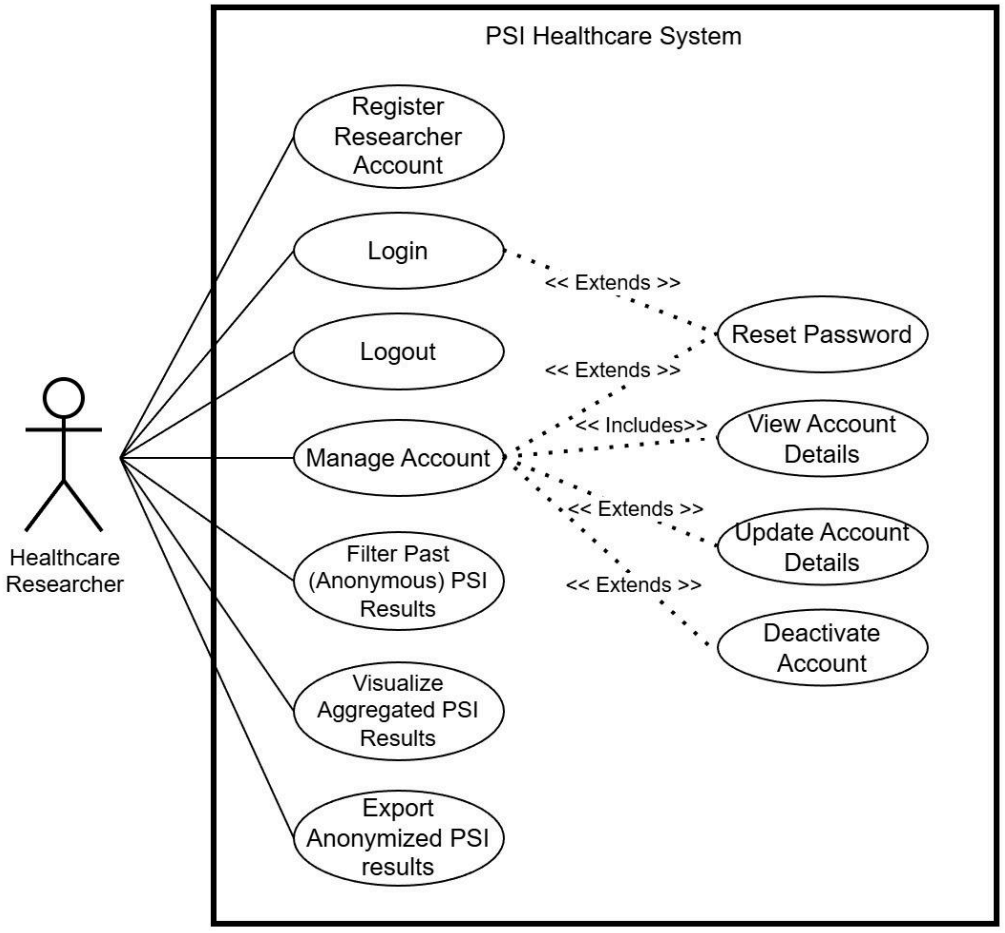
Alternative/Exceptional Flows:

1. If validation fails, the system displays an error message prompting correction.

2. If the update process fails due to a system error, the system logs the error and notifies the user.

8.1.5 Health Researcher

8.1.5.1 Use Case Diagram



8.1.5.2 User Stories

No.	Healthcare Researcher User Stories
1	As a health researcher,I want to visualize the aggregated PSI results in dashboards, so that I can better analyze patterns and trends without accessing raw patient data.
2	As a health researcher, I want to filter PSI results based on specific criteria (e.g., age, location, disease type), so that I can focus my research on targeted populations.
3	As a health researcher, I want to export anonymized PSI results into standard formats (CSV, JSON), so that I can integrate them with existing research tools and workflows.
4	As a healthcare researcher, I want to register for an account using my professional details and email, so that I can securely access the PSI platform and its research tools.
5	As a healthcare researcher, I want to log in using my registered credentials, so that I can securely access my research dashboard.
6	As a healthcare researcher, I want to log out of my account, so that I can ensure my data and sessions remain private when I'm done working.
7	As a healthcare researcher, I want to reset my password when I forget it, so that I can regain access to my account without losing my saved settings or data.
8	As a healthcare researcher, I want to view my account information, so that I can verify my profile and ensure all details are accurate.
9	As a healthcare researcher, I want to update my account information, so that I can keep my contact details and credentials up to date.
10	As a healthcare researcher, I want to deactivate my account, so that I can permanently stop using the platform and remove my access to the system.

8.1.5.3 Use Case Description

Name: Visualize Aggregated PSI Results in Dashboards	ID: R01
Stakeholders and goals: Researchers want to analyze results without accessing raw data.	
Description: Generates dashboards showing summary statistics and patterns from PSI results.	
Actors: Healthcare Researcher	
Trigger: Researcher opens “Analytics Dashboard.”	
Normal Flow: 1. System retrieves aggregated PSI results. 2. Displays data in visual formats (graphs, charts). 3. Researcher filters and explores data trends.	
Sub-Flows: Visualization rendering.	
Alternative/Exceptional Flows: If no data available, display “No recent PSI results.”	

Name: Filter PSI Results by Specific Criteria	ID: R02
Stakeholders and goals: Researchers want to focus their analysis on targeted populations or diseases.	
Description: Allows filtering PSI results by parameters such as age, location, or disease type.	
Actors: Healthcare Researcher	
Trigger: Researcher applies filter options.	
Normal Flow: 1. The researcher selects filter criteria. 2. The system applies filters to aggregated results. 3. Display updates to reflect refined dataset.	
Sub-Flows: Query processing.	
Alternative/Exceptional Flows: If invalid filters are used, system resets to	

default dataset view.

Name: Export Anonymized PSI Results13.4	**ID: R03**
Stakeholders and goals: Researchers want to use PSI outputs with external analytical tools.	
Description: Allows exporting aggregated, anonymized PSI results in standard data formats (CSV, JSON).	
Actors: Healthcare Researcher	
Trigger: Researcher selects “Export Results.”	
Normal Flow: 1. The researcher chooses the format (CSV/JSON). 2. The system generates files and anonymizes sensitive identifiers. 3. Download or export confirmation provided.	
Sub-Flows: Data anonymization and format conversion.	
Alternative/Exceptional Flows: If export fails, system prompts retry or displays error message.	

Name:Register Researcher Account	**ID: R04**
Stakeholders and goals: Healthcare Researcher wants to register for an account so they can access PSI result data.	
Description: Allows new healthcare researchers to create an account using their email and password to access healthcare risk assessment services.	
Actors: Patient	
Trigger: The patient selects the “Register” option on the login page.	
Normal Flow: 1. The healthcare researcher clicks on “Register”. 2. The system prompts for email, password and password confirmation. 3. Healthcare researcher clicks “Submit”. 4. The system validates the input. 5. The account is created and confirmation is sent to the patient.	

Sub-Flows: Email verification process.
Alternative/Exceptional Flows: ● If the email is already in use, the system displays an error message and requests a different email. ● If the entered password and password confirmation do not match, display an error message informing users that the two passwords do not match. ● If the entered passwords match but do not meet the password requirements, display an error message informing users of the password requirements.

Name: Login to Researcher Account	**ID: R05**
Stakeholders and goals: Healthcare researchers want to log in securely to their account.	
Description: Allows registered healthcare researchers to log in to their account using valid credentials.	
Actors: Healthcare Researcher	
Trigger: Healthcare Researcher clicks “Login” after entering their credentials.	
Normal Flow: 1. The healthcare researcher enters an email and password. 2. Healthcare researcher clicks “Submit”. 3. System validates credentials. 4. The system grants access and loads the dashboard.	
Sub-Flows: Session management.	
Alternative/Exceptional Flows: ● If credentials are invalid, display “Incorrect email or password.” ● If the account is suspended or deactivated, display: “Your account has been restricted. Contact the system administrator.”	

Name: Logout from Researcher Account	**ID: R06**
Stakeholders and goals: Healthcare Researcher wants to log out to maintain account security.	
Description: Ends the user session and redirects the patient to the homepage.	

Actors: Healthcare Researcher
Trigger: Healthcare Researcher clicks “Logout.”
Normal Flow: 1. Healthcare Researcher clicks logout. 2. System ends the active session. 3. System redirects to the login page.
Sub-Flows: Session termination
Alternative/Exceptional Flows: None

Name: Reset Healthcare Researcher Account Password	**ID: R07**
Stakeholders and goals: Healthcare Researcher wants to regain access when they forget their password.	
Description: Allow Healthcare Researcher to reset their password securely through their registered email.	
Actors: Healthcare Researcher	
Trigger: Healthcare Researcher clicks “Forgot Password.”	
Normal Flow: 1. Healthcare Researcher requests password reset. 2. System prompts for registered email. 3. The system sends a reset link to the email. 4. The Healthcare Researcher sets a new password. 5. System confirms password change.	
Sub-Flows: Email verification and token validation.	
Alternative/Exceptional Flows: If the email is not registered, show “Account not found.”	

Name: View Healthcare Researcher Account Information	**ID: R08**
Stakeholders and goals: Healthcare Researcher wants to view their own account details, such as name, email, role, and contact information.	

Description: Allows Healthcare Researcher to view their account information so that they can verify that the information is correct.
Actors: Healthcare Researcher
Trigger: Healthcare Researcher selects the “My Account” option from their dashboard navigation menu.
Normal Flow: 1. The healthcare researcher logs into the admin dashboard. 2. The healthcare researcher clicks the “My Account” or “Profile” tab. 3. The system retrieves the healthcare researcher’s stored account details from the database. 4. The system displays relevant information 5. The healthcare researcher reviews their account details.
Sub-Flows: Email verification and token validation.
Alternative/Exceptional Flows: If the system cannot retrieve the account details (e.g. database error), display: “Unable to load account details. Please try again later.”

Name: Update Healthcare Researcher Account Information	**ID: R09**
Stakeholders and goals: Healthcare Researcher wants to update their own account information, such as email, contact details, or password, so that they can keep their profile current and maintain secure access to the system.	
Description: Allow the Healthcare Researcher to edit and update their personal account details from within the admin dashboard to ensure that their contact and authentication information remain accurate.	
Actors: Healthcare Researcher	
Trigger: The Healthcare Researcher selects the “Edit Account” option from the profile page.	
Normal Flow: 1. The healthcare researcher navigates to the “My Account” section. 2. The system displays the current account information. 3. The healthcare researcher edits one or more fields. 4. The system validates all input fields for correctness and format.	

5. The healthcare researcher confirms and submits the changes.
6. The system updates the account information in the database.
7. The system displays a confirmation message indicating successful update.

Sub-Flows: None

Alternative/Exceptional Flows:
- If input validation fails (e.g. invalid email format, weak password), the system displays an error message and prevents submission.
- If the database update fails, display: “Unable to update account information. Please try again later.”
- If the session expires before submission, the system prompts for re-login before proceeding.

Name: Delete Researcher Account	**ID: R10**

Stakeholders and goals: Healthcare Researcher wants to permanently deactivate and delete their account from the platform when they no longer wish to view PSI data from the application.

Description: Allows Healthcare Researchers to perform deletion of their account from the system.

Actors: Healthcare Researcher

Trigger: The Healthcare Researcher selects the “Delete Account” option from the account settings.

Normal Flow:
1. The healthcare researcher navigates to the account settings page.
2. The system displays an option to delete the healthcare researcher’s account.
3. The healthcare researcher clicks “Delete Account.”
4. The system prompts for confirmation, “Are you sure you want to delete this account? This action cannot be undone.”
5. The healthcare researcher confirms the deletion request.
6. The system deletes all related data, logs the action, and terminates the healthcare researcher’s access.

7. The system displays a confirmation message and logs the user out.
Sub-Flows: None
Alternative/Exceptional Flows: ● If the healthcare researcher cancels at the confirmation step, the system aborts the deletion process. ● If the deletion process fails, the system aborts the deletion process and displays an error message, “Unable to delete account at this time. Please try again later or contact an administrator.”

8.2 Non-Functional Requirements

8.2.1 Performance

The system shall ensure that Private Set Intersection (PSI) computations for datasets complete within seconds, providing near real-time results to patients. The application must be capable of supporting at least 100 concurrent active users without experiencing any performance degradation. Additionally, hospitals and healthcare providers must be able to efficiently handle a minimum of 10 simultaneous patient PSI requests without compromising response times or accuracy.

8.2.2 Security

The PSI protocol implementation must utilize the Diffie-Hellman cryptographic method to ensure secure set intersections. The system shall implement Role-Based Access Control (RBAC) to strictly restrict access based on user roles, including patient, hospital, administrator, researcher, and system security personnel. All PSI operations and sensitive actions must be comprehensively logged in with secure, tamper-evident audit trails to maintain accountability and traceability. To protect system integrity, the application must not display raw or detailed error messages to end users; instead, error handling should provide user-friendly messages while logging detailed technical information for administrators.

8.2.3 Usability

The user interface design shall clearly present PSI results in an understandable and user-friendly format, enabling patients to comprehend their genetic risk assessments without requiring technical expertise. The UI should be intuitive enough for users to navigate and utilize the system easily without extensive learning or training. Clear visual indicators must be provided to inform users when processes are being executed, such as authentication, data upload, or PSI computation. The application must be fully responsive and functional across desktop and mobile devices, supporting all modern web browsers to ensure accessibility for diverse user populations.

8.2.4 Reliability

Users should be able to access and use the system 98% of the time without experiencing failures or service interruptions. In the event that the system experiences a failure, recovery mechanisms must be in place to restore services promptly. The system must handle failures and errors gracefully, presenting proper and meaningful error messages to users while maintaining data integrity. Daily

automated backups must be performed to safeguard all system data, with full system recovery capabilities that can be executed within a few hours to minimize downtime.

8.2.5 Scalability

The system architecture must support an increasing number of users across all roles—patients, hospitals, and researchers—without significant degradation in performance or user experience. The PSI computation engine must be optimized to process larger gene sets efficiently, with computation times that scale appropriately with dataset size. Database and storage systems must be designed to be scalable, accommodating long-term growth in user data, genetic information, and audit logs without requiring major architectural changes.

8.2.6 Maintainability

The system must employ a modular design approach that supports component-level updates and enhancements without requiring full system redeployment, thereby reducing maintenance complexity and downtime. Hospital gene databases must be updatable through the administrative interface without necessitating system downtime, ensuring continuous availability while maintaining current research data.

8.2.7 Availability

The system must maintain 24/7 availability to ensure that patients can access their genetic risk assessment services at any time. Any scheduled maintenance activities must be announced to users in advance and performed during off-peak hours to minimize disruption. Critical system components must incorporate failover mechanisms to ensure uninterrupted service in the event of component failures. Real-time monitoring tools must be deployed to detect outages or performance issues and immediately notify system administrators, enabling rapid response to potential problems.

8.2.8 User Interface (UI) Requirements

No.	UI Requirement
1.	**Transparency in PSI Operations** ● The system must clearly communicate to users when PSI computations are taking place, displaying visual indicators such as progress bars or loading animations with messages like "Securely computing your risk assessment...". ● Patients must be informed that their complete genetic data is never revealed to the hospital, and hospitals must be assured that patient genetic profiles remain confidential. ● Results screens should include brief explanations of how PSI protects privacy, using accessible language without technical jargon For patients, risk assessment results must be presented with clear percentage values (e.g., "15% increased risk") accompanied by explanatory text about what the percentage means and recommended next steps.
2.	**Intuitive Data Upload and Management** ● File upload interfaces must support common genetic data formats (e.g., 23andMe, AncestryDNA raw data) with clear instructions and format validation. ● Drag-and-drop functionality should be provided for genetic data uploads with visual feedback during the upload process. ● Users must receive immediate validation feedback if uploaded files are in incorrect formats or contain errors, with specific guidance on how to correct issues. ● The system must allow patients to easily delete their uploaded genetic data after receiving results, with prominent "Delete My Data" buttons and confirmation dialogs Patients should be able to view their assessment history in a timeline or list format, with the ability to filter by disease type or date.

3.	**Role-Based Interface Customization** ● Each user role (Patient, Hospital, System Administrator, System Security, Health Researcher) must have a customized dashboard that presents role-relevant information and actions prominently. ● Navigation menus and available features must be tailored to the permissions and responsibilities of each user role, hiding unnecessary options. ● Hospital administrators must have dedicated interfaces for managing disease-gene databases, with clear categorization by disease type (cardiovascular, oncological, neurological, etc.). ● System administrators and security personnel must have access to monitoring dashboards with real-time system status, audit logs, and security alerts. ● Advanced users should have the option to customize their dashboard layout and information density according to their preferences.
4.	**Reduce Cognitive Load** ● The interface should minimize the need for users to remember previous actions, inputs, or results by maintaining context across screens and sessions. ● Complex workflows (such as multi-disease risk assessment) should be broken down into clear, sequential steps with progress indicators showing "Step 1 of 4" or similar Important information should be organized hierarchically, with critical data (e.g., high-risk results) displayed more prominently than supplementary details. ● The system should provide contextual help and tooltips for technical terms (e.g., "PSI," "genetic markers," "risk coefficient") that may be unfamiliar to patients. ● Auto-save functionality must be implemented for forms and data entry to prevent loss of work if users navigate away or experience connection issues.

5.	**Consistent Design and Navigation** ● The application must maintain consistent visual design elements (colors, fonts, button styles, icons) across all pages and user roles to create a cohesive experience. ● Navigation elements (menus, breadcrumbs, back buttons) must be positioned consistently throughout the application, with clear indicators of the current page or section. ● Interactive elements must provide consistent feedback: buttons should have hover, active, and disabled states; form fields should highlight on focus; links should be visually distinguishable. ● Error messages and validation feedback must follow consistent formatting and placement patterns, using standard colors (red for errors, green for success, yellow for warnings). ● The design should follow established healthcare application conventions where users expect certain patterns (e.g., red for high risk, green for low risk).
6.	**Accessibility and Responsiveness** ● The application must be fully responsive and functional across desktop computers, tablets, and mobile devices with appropriate layouts for different screen sizes. ● The interface must comply with Web Content Accessibility Guidelines (WCAG 2.1 Level AA) to ensure usability for users with disabilities. ● Text must be legible with sufficient color contrast ratios (at least 4.5:1 for normal text, 3:1 for large text) and support browser zoom up to 200%. ● All interactive elements must be keyboard-navigable for users who cannot use a mouse, with visible focus indicators. ● Images and icons must include descriptive alt text, and critical information should not rely solely on color to convey meaning.

7.	**User Control and Flexibility** ● Users must be able to easily undo or cancel unintended actions through prominent "Cancel," "Go Back," or "Undo" buttons before final submission. ● Confirmation dialogs must be presented for destructive actions (e.g., deleting genetic data, canceling appointments, deactivating accounts) with clear descriptions of consequences. ● The system should allow users to save incomplete work and return later, particularly for multi-step processes like comprehensive risk assessments. ● Patients should have control over their data, with easy-to-find options to export results as PDF or images, view data usage logs, and manage privacy settings. ● Search and filter functionality must be provided for interfaces with large datasets (e.g., disease gene databases, appointment histories, audit logs).
8.	**Clear Error Handling and Security Feedback** ● Error messages must be user-friendly and actionable, avoiding technical jargon and providing specific guidance on how to resolve issues (e.g., "The uploaded file must be in .txt format. Please convert your file and try again."). ● The system must not display detailed technical error messages or stack traces to end users, as these could expose security vulnerabilities. ● Security-related actions (login, password reset, data deletion) must provide clear feedback about success or failure without revealing sensitive information (e.g., "Invalid credentials" rather than "Incorrect password"). ● Session timeout warnings should appear before automatic logout, giving users the opportunity to extend their session if actively working. ● The system must clearly indicate when network requests are in progress, when operations have completed successfully, and when errors occur requiring user attention.

9 Future Enhancements

9.1 Overview

This section outlines a strategic enhancement planned for future phases of the PSI Healthcare Application: the Family Access Feature. While the current project scope focuses on delivering core PSI functionality for direct patient-hospital interactions, the Family Access feature represents a natural evolution that addresses real-world accessibility challenges in healthcare technology adoption. This enhancement is designed to expand the system's utility to vulnerable populations, particularly elderly patients who may require assistance in navigating digital healthcare platforms, while maintaining the rigorous privacy guarantees established by the PSI protocol.

The Family Access feature has been intentionally scoped as a future enhancement rather than a core requirement to ensure that the development team can concentrate on perfecting the fundamental PSI implementations, security infrastructure, and user workflows in the initial release. Once the foundation is stable and thoroughly tested, this accessibility-focused enhancement can be integrated systematically without compromising the core system's integrity.

9.2 Problem Statement

Primary Challenges Addressed:

1. ***Digital Literacy Barriers:*** Elderly patients often possess limited technological proficiency, making independent use of web-based healthcare applications challenging despite having legitimate need for genetic risk assessment services.
2. ***Medical Information Complexity:*** Genetic risk assessments involve specialized medical terminology and statistical concepts that can be difficult for non-expert users to interpret correctly without assistance.
3. ***Healthcare management Support:*** Family members frequently serve as information healthcare coordinators for elderly relatives but lack systematic tools to support this role while respecting patient privacy.
4. ***Accessibility and Inclusion:*** Current healthcare technology often fails to accommodate users who require assistance, effectively excluding vulnerable populations from benefiting from advanced diagnostic capabilities like PSI-based risk assessment.
5. ***Aging Population Trends:*** With global demographic shifts toward aging populations, healthcare systems increasingly need solutions that

accommodate elderly users' technology and comprehension needs while maintaining security and privacy standards.

9.3 Patient User Stories Integration

Existing User Story	Family Access Extension	Integration Type
US-P01-P04: Patient authentication (register, login, logout, password reset)	Family members use the same authentication system with separate accounts.	**Shared Infrastructure**
US-P05: Patient uploads genetic data securely	The system ensures caregivers never access this data; only patients have genetic data permissions. **US-P27** enforces this architectural constraint.	**Privacy Enforcement**
US-P06-P08: Patient views risk results in simple, clear format with explanations	**US-F02:** Caregivers view the same simplified risk presentation (disease name, risk percentage, explanation) but without access to underlying genetic data.	**Extended Viewing**
US-P09: Patient deletes genetic data	When a patient deletes genetic data, any associated family access relationships are automatically terminated to maintain data integrity.	**Cascading Effect**
US-P11: Patient views assessment history	**US-F04:** Caregivers view patient's assessment history (with permission) to help track risk trends over time.	**Extended Viewing**
US-P12: Patient selects multiple diseases for assessment	**US-F03:** Caregivers can initiate multi-disease assessments on patient's behalf (if granted permission) using patient's stored genetic data.	**Delegated Action**
US-P13: Patient exports results as PDF/image	**US-F04:** Caregivers can export results (with permission) to share with patients or discuss with family.	**Extended Export**
US-P14-P16: Patient account management (view details, update info, delete account)	**US-P23:** Patient reviews family access requests and approves/denies them as part of the account management dashboard.	**New Management Function**

US-P16: Patient deletes account permanently	When a patient account is deleted, all family access relationships are automatically terminated and caregiver access immediately revoked.	**Cascading Effect**
US-P20: Patient receives appointment notifications	**US-F05** (acceptance criteria): Caregivers receive notifications when new risk results are available (separate notification stream, configurable by patient).	**Parallel Notification**
US-P22: Patient searches for specific diseases or categories	**US-F03:** When a caregiver initiates assessment, they use the same disease search functionality to select which risks to assess.	**Shared Functionality**

9.4 Hospital User Stories Integration

Existing User Story	Family Access Extension	Integration Type
US-H02: Hospital performs PSI computation to provide risk calculations	When a caregiver initiates assessment (**US-F03**), the hospital's PSI computation uses the patient's stored genetic data—no new genetic uploads required.	**Reused PSI Infrastructure**
US-H04: Hospital processes multiple patient requests efficiently	The system tracks whether requests originated from patients or caregivers for hospital records and workload management.	**Enhanced Tracking**
US-H11: Hospital categorizes disease genes by disease type	**US-F03:** Caregivers use the same disease categorization when selecting which risk assessments to initiate.	**Shared Categorization**
US-H15: Hospital views all scheduled appointments with patients	**US-H25:** Hospital sees assessments marked as “Initiated by: Patient” or “Initiated by: Caregiver [Name]” for consultation context and patient communication.	**Context Information**
US-H23: Hospital searches for specific genes in database	When processing caregiver-initiated assessments (**US-F03**), hospitals use the same gene search functionality in PSI computation.	**Reused Functionality**

9.5 System Administrator User Stories Integration

Existing User Story	Family Access Extension	Integration Type
US-A02: System admin maintains audit logs of all calculations	**US-A20:** Admin views family access audit logs (who accessed what, when) as part of comprehensive system monitoring.	**Extended Audit Capability**
US-A05: Admin views all registered users	**US-A20:** Admin views family access relationships as part of user oversight (which caregivers have access to which patients) in the same user management interface.	**Enhanced User Management**
US-A06: Admin resets passwords for locked-out users	Admin may need to create emergency family access (**US-A19**) if the patient is locked out and needs a caregiver to help manage account recovery.	**Emergency Support**
US-A07: Admin monitors system performance and data usage	**US-A20:** Admin monitors family access feature performance (relationship queries, permission checks, data filtering operations) as part of overall system metrics.	**Performance Monitoring**
US-A10: Admin generates monthly usage and performance reports	**US-A20:** Family access analytics (adoption rate, active relationships, permission distributions) included in monthly reports.	**Reporting Integration**
US-A11: Admin sets rate limits on PSI computations	When a caregiver initiates assessment (**US-F03**), rate limits apply to prevent abuse; caregivers share the patient's rate limit quota.	**Applied Rate Limiting**
US-A12: Admin views detailed user account information	**US-A20:** Admin views family access relationships as part of user account details (who they've granted access to, who has access to them).	**Enhanced Account View**
US-A13: Admin updates user account information	**US-A19, US-A21:** Admin can create relationships and modify permissions as part of account support services.	**Extended Account Management**

US-A14: Admin suspends/deactivates accounts that violate terms	**US-A22:** Admin suspends family access relationships (not entire accounts) for investigation; can escalate to account suspension if needed.	**Granular Suspension**
US-A15: Admin permanently deletes user accounts	When admin deletes a patient account (**US-A15**), all family access relationships are automatically terminated (**cascades to US-A23 termination logic**).	**Cascading Deletion**
US-A16: Admin views analytics on appointments	**US-A20:** Admin views family access analytics alongside appointment analytics in a unified dashboard.	**Analytics Integration**

9.6 System Security User Stories Integration

Existing User Story	Family Access Extension	Integration Type
US-S02: Enforce encryption of all data at rest and in transit	Caregiver data access uses the same encryption standards; genetic data remains encrypted and inaccessible to caregivers (US-P27 enforces filtering).	**Applied Security Standard**
US-S03: Enforce role-based access control (RBAC)	**US-P24:** Patient-controlled permissions add a new dimension to RBAC—patients define caregiver role capabilities within the existing RBAC framework.	**Extended RBAC**
US-S04: Monitor PSI logs for anomalies	**US-A20:** System monitors for suspicious family access patterns (e.g., caregiver accessing many patients, high-frequency access, unusual locations).	**Extended Monitoring**
US-S05: Receive automated alerts for suspicious PSI activities	**US-A20:** System generates alerts for suspicious family access patterns (same alerting infrastructure, new detection rules).	**Extended Alerting**
US-S06: Generate compliance and audit reports	**US-A20:** Family access activities included in compliance reports; demonstrates privacy protection for caregivers accessing patient data.	**Expanded Compliance**
US-S07: Implement secure logging and audit trails	**US-P25, US-A20:** Audit trails cover all caregiver actions (view results, initiate	**Extended Audit Trails**

	assessments, export data) with the same security standards.	
US-S08: Periodically review and update security policies	Family access feature subject to same security policy reviews; policies cover caregiver access controls and genetic data isolation.	**Policy Coverage**
US-S09: Conduct regular penetration tests	Penetration testing includes family access attack vectors: privilege escalation attempts, data filtering bypass, permission circumvention.	**Expanded Testing Scope**
US-S10: Isolate and contain compromised accounts	**US-A22:** Admin can suspend family access relationships if the caregiver account is compromised without affecting the patient's account.	**Isolated Containment**
US-S11: Implement MFA for hospital administrator accounts	The system can optionally require MFA for caregivers accessing sensitive risk data (configurable security enhancement).	**Optional Enhanced Security**

9.7 Healthcare Researcher User Stories Integration

Existing User Story	Family Access Extension	Integration Type
US-R05: Researcher visualizes aggregated PSI results	Family access relationships are anonymized in research data; researchers cannot identify caregiver-patient connections.	**Privacy-Preserved Aggregation**
US-R06: Researcher filters PSI results by criteria	Researchers can filter to see which assessments were patient-initiated vs. caregiver-initiated (without identifying specific individuals).	**Research Insight**
US-R07: Researcher exports anonymized PSI results	Exported data includes indicator of initiation source (patient/caregiver) but no identifying information about family relationships.	**Enhanced Data Export**

10 Reference

NUHS App (August 12, 2025). *NUHS | National University Health System*. Retrieved October 17, 2025 from https://www.nuhs.edu.sg/patient-care/nuhs-app

About HealthHub (n.d.). *HealthHub.* Retrieved October 27, 2025 from https://www.healthhub.sg/about-healthhub

What we do (2015-2025). *Genomapp*. Retrieved October 29, 2025 from https://genomapp.com/en/

Our Services (2024). *Genexsure*. Retrieved October 29, 2025 from https://genexsure.com/patients-services/

Your health starts in your genes (2025). Invitae. Retrieved October 31, 2025 from https://www.invitae.com/us/patients-and-individuals?tab=get-a-virtual-consult

PDPA Overview (November 3, 2023). *PDPC | Personal Data Protection Commission*. Retrieved November 4, 2025 from https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine, 129(1)*, 104130. https://doi.org/10.1016/j.compbiomed.2020.104130

Huberman, B. A., Franklin, M. K., & Hogg, T. (1999). Enhancing privacy and trust in electronic communities. *Electronic Commerce.* https://doi.org/10.1145/336992.337012