Software Requirements Documentation

for

Leveraging Digital Phenotyping to Support Patients with Glaucoma

Prepared by Stellina Ao, Luis Ayala-Saldivar, Edson Castellanos, Mengying Chen, John Huang, Jooeun Jeon, Desiree Ramirez, Ashley Tran, Thang Tran

Sponsored by The National Institute of Health (NIH), CSUBIOTECH

Created November 30, 2023
Last Edited December 8, 2023

Table of Contents

Revision History

Name	Date	Reason for Changes	Version
Stellina Ao, Luis Ayala-Saldivar, Edson Castellanos, Mengying Chen, John Huang, Jooeun Jeon, Desiree Ramirez, Ashley Tran, Thang Tran	12/06/2023	Initial Draft	1.0

1. Introduction

1.1 Purpose

This document provides an overview of the requirements for the mobile application using digital phenotyping to monitor glaucoma. This document will also cover concepts that are important in understanding the operation of the system.

1.2 Intended Audience and Reading Suggestions

This document will be useful for the software development team, testing team, project managers, and the system's potential users. This document is best read in various ways depending on the role.

Development Team: must understand product requirements and implementation

Testing Team: must understand product purpose and requirements

Project Manager: must understand product purpose and requirements

Users (Patients): must understand product purpose and user interface paradigms

Users (Physicians): must understand product purpose and user interface paradigms

1.3 Product Scope

This mobile application characterizes user’s driving behaviors and relates them to the progression of glaucoma. In addition, the mobile application will detect and assess whether the patient's glaucoma is progressing too quickly and inform the patient's physician and the Department of Motor Vehicles (DMV) in certain situations. The mobile application will *not* act as a diagnostic or cure for glaucoma but as a tool to monitor glaucoma.

1.4 Definitions, Acronyms, and Abbreviations

Refer to *Appendix A*.

2. Overall Description

2.1 System Analysis

The application is designed for primary physicians to monitor the progression of glaucoma within their patients through their driving behaviors. The application will collect data from smartphones with sensors such as a triaxial accelerometer and gyroscope (measuring device motion and rotation, respectively). The data will be used to create driving statistics aiding physicians in evaluating the patient's ability to drive safely. If the patient's condition prevents them from driving safely, the application will notify the patient and their physician.

2.2 Product Perspective

The application operates autonomously and does not depend on other applications or the active engagement of users.

2.3 Product Functions

2.3.1 Registration (patient/physician): Sign up for the application by creating an account as either a physician or patient with a username and password.
2.3.2 Login page: Login either as a patient or a physician, which will direct to the appropriate portal.
2.3.2 Homepage (Patient): The homepage for patients displays the list of trips the patient has made with the corresponding distance, route, and time of each trip. Additional triaxial accelerometer and gyroscope driving information are collected and recorded in the application's background, such as acceleration, braking, and cornering.
2.3.3 Homepage (physician): The homepage for physicians will comprise a list of registered patients and their corresponding processed driving data, such as speeding score, average length of trips, and overall driving score. The homepage should allow clicking on a patient record that will redirect to the Patient Information Page for more expansive patient-driving data.
2.3.4 Individual Patient Information Page: Physicians will have access to each patient's processed sensor data and calculated scores. Driving information from sensors and detailed driving scores calculated for notable driving metrics will be displayed.
2.3.5. Personal Information Page: This page displays the user information obtained during the registration, such as username and password. This page also enables users to add or change a physician. Users may also change the measurement unit for mileage (km/mi) and time (24/12 hours).
2.3.6 Help Page: Displays the information about the app and contact information for customer support

2.4 User Classes and Characteristics

The application is designed with two main user interfaces (UIs): one for patients and another for primary care physicians.

Patients can access a simple screen with their drive history, including only the drive distance, length, and routes. The drive history records should be updated after each trip. Patients should also have access to a profile screen where the unit of measurement for the drive metrics (e.g., km/mi, 12-/24-hour) can be customized and viewed by the physician(s) with access to their processed driving behaviors. Patients' screens will be kept very simple with no detailed driving score to ensure that data displayed on the app does not affect patients' driving behaviors. Patients cannot access their detailed drive history and scores.

The physician's view provides a more comprehensive overview. It offers detailed information about their patients, including data such as driving statistics and the patients' overall driving score. Driving score is calculated for each category: acceleration, braking, speeding, distraction, and cornering. The score enables physicians to assess whether a patient's condition enables them to drive safely.

2.5 Operating Environment

The application will utilize the patient's mobile device (iOS/Android).

2.6 Design and Implementation Constraints

One such constraint involves the system's vulnerability to weak network connectivity. The application may face difficulty accurately tracking patients' movements in unstable network conditions. Another constraint involves the use of modern smartphones. Patients will need smartphones with a triaxial accelerometer and gyroscope to use the application.

2.7 User Documentation

The user documentation cannot be accessed by patients alone. The patient's driving data is stored in secure data with an identification number (ID). Physicians can access the data of each patient using their ID and can use the data to check the patient's current condition.

2.8 Assumptions and Dependencies

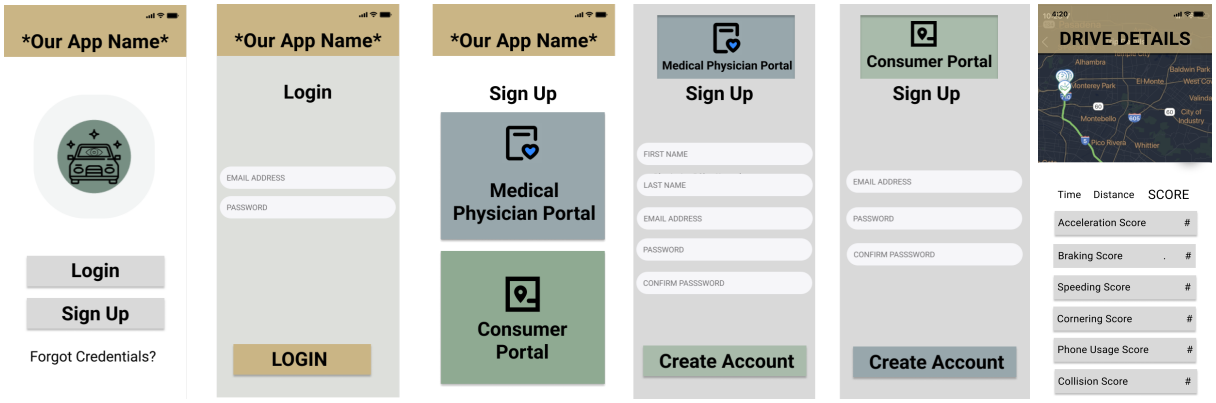
2.8.1 Assume cellular devices are connected to the network
2.8.2 Assume cellular devices are equipped with sensors such as a triaxial accelerometer, gyroscope, and magnetometer

2.9 Apportioning of Requirements

None available at this time, as the application is still in the early development stage

3. External Interface Requirements

3.1 User Interfaces



3.1.1 The application must display user interfaces (UI) using a color palette with high contrast
3.1.3 The application must display large fonts and buttons for patient UIs
3.1.3 The application must present a home page when it is loaded
3.1.4 The application must present a UI for log-in, sign-up, and reset credentials options
3.1.5 The application must present a UI to log-in or sign-up as a patient or physician
3.1.6 The application must not present a UI allowing a patient to view their driving statistics
3.1.7 The application must enable the physician to view the patient's driving statistics

3.2 Hardware Interfaces

3.2.1 The application must support iOS and Android platforms
3.2.2 The application must operate and collect data on smartphones with sensors such as accelerometers, gyroscopes, magnetometers, and GPS
3.2.3 The application requires a smartphone with network capabilities

3.3 Software Interfaces

3.3.1 The application must utilize the cloud data storage platform DataHub by Damoov

3.4 Communications Interfaces

3.4.1 The application requires a stable network connection
3.4.2 The application must send encrypted data to DataHub
3.4.3 The application must decrypt data received from DataHub

4. Requirements Specification

4.1 Functional Requirements

4.1.1 Application Requirements

- 4.1.1.1 The application must support iOS and Android devices
- 4.1.1.2 The application must include an interface to validate credentials
  - 4.1.1.2.1 The application must deactivate all functions without valid credentials.
- 4.1.1.3 The application must include an interface to register an account
  - 4.1.1.3.1 The application must include designated fields for entering a username and password, and it must incorporate a password confirmation feature.
  - 4.1.1.3.2 The application must include a confirmation message for successful registration
- 4.1.1.4 The application must include an interface to view a medical physician portal and a patient's portal
- 4.1.1.5 The application must include an interface to view a configuration screen to inform users of the data the application will collect from them
- 4.1.1.6 The application must include an interface to view the user driving metric
  - 4.1.1.6.1 The application must include an interface to view the user mileage, route, and time-driven for the patient
- 4.1.1.7 The application must include an interface to view the user weekly, monthly, and yearly driving scores
- 4.1.1.8 The application must include an interface for physicians only
  - 4.1.1.8.1 The application must not include the user route
  - 4.1.1.8.2 The application must display data of the driving behavior and habits of the user
  - 4.1.1.8.3 The application must include an interface to view patients, glaucoma risk factor, and overall safety score
  - 4.1.1.8.4 The application must include an interface to view the user's average speed, acceleration, braking, cornering, and phone usage
- 4.1.1.9 The application must include an interface to logout
  - 4.1.1.9.1 The application must hide functionalities when the user logs out
- 4.1.1.10 The application must provide a navigation to the home page

4.2 External Interface Requirements

4.2.1 User Interfaces

- 4.2.1.1 Registration
  - 4.2.1.1.1 The application must provide users without accounts a way to sign up
  - 4.2.1.1.2 The application must include input boxes for username and password

4.2.1.1.3 The application must display a confirmation message once an account is formed

4.2.1.2 Credential Verification

4.2.1.2.1 The application must verify the username and password of the user

4.2.1.2.2 The application must input boxes for username and password

4.2.1.2.3 The application must display all functionalities

4.2.2 Software Interfaces

4.2.2.1 Damoov Datahub & AWS

4.2.2.1.1 The application must interface with Damoov DataHub and AWS to store user information

4.2.2.1.2 The application must query according to the data accessed

4.2.2.1.3 The application must output results relevant to the application

4.3 Logical Database Requirements

4.3.1 Types of information used

4.3.1.1 Physicians Data

4.3.1.1.1 Username

4.3.1.1.2 Password

4.3.1.1.3 Email

4.3.1.1.4 Status of user

4.3.1.1.5 Profile

4.3.1.1.6 List of physicians patients

4.3.1.1.7 Patient’s glaucoma risk factor

4.3.1.1.8 Patient's overall safety score

4.3.1.1.9 Patient’s driving statistics

4.3.1.2 Patients Data

4.3.1.2.1 Username

4.3.1.2.2 Password

4.3.1.2.3 First Name

4.3.1.2.4 Last Name

4.3.1.2.5 Email

4.3.1.2.6 Status of user

4.3.1.2.7 Profile

4.3.1.2.8 Patient’s driving statistics

4.3.1.2.9 Overall safety score

4.3.1.3 Driving Data

4.3.1.3.1 Patient’s processed driving statistics

4.3.2 Frequency of use

4.3.2.1 Physicians Data

4.3.2.1.1 The application must access physicians data when validating login information

4.3.2.1.2 The application must add to physicians data when creating a new account

4.3.2.1.3 The application must access physicians data when displaying the user driving metrics

4.3.2.1.4 The application must access physicians data when displaying patients driving metrics

4.3.2.1.5 The application must add to physicians data when adding a new patient

4.3.2.2 Patients Data

4.3.2.2.1 The application must access patients data when validating login information

4.3.2.2.2 The application must add to patients data when creating a new account

4.3.2.2.3 The application must access patients data when displaying users driving metrics

4.3.2.2.4 The application must add to patients data when a user drives

4.3.2.3 Drive Data

4.3.2.3.1 The application must access drive data when displaying users driving metrics

4.3.2.3.2 The application must add to drive data when a user drives

4.3.3 Accessing capabilities

4.3.3.1 Physicians Data

4.3.3.1.1 The application may access user data exclusively via methods specifically crafted to address the situations outlined in 4.3.2.1

4.3.3.2 Patients Data

4.3.3.2.1 The application may access physicians data exclusively via methods specifically crafted to address the situations outlined in 4.3.2.2

4.3.3.3 Drive Data

4.3.3.3.1 The application may access patients data exclusively via methods specifically crafted to address the situations outlined in 4.3.2.3

4.3.4 Integrity constraints

4.3.4.1 The application must guarantee that only users who are registered have access to its functionality

4.3.4.2 The application must incorporate measures to enforce strong passwords

4.4 Design Constraints

4.4.1 Internet connectivity

4.4.1.1 The application must be run with reasonably stable internet access, as slow and inconsistent internet may cause a lag in services and unacceptable performance.

4.4.2 Mobile access

4.4.2.1 The application must have access to an iOS or Android device to run because it is a mobile application
4.4.2.2 The iOS or Android device must include sensors for the user driving data collection
4.4.2.3 Accessing the application via mobile device may limit the text due to large fonts

5. Other Nonfunctional Requirements

5.1 Performance Requirements

5.1.1 The system must support data storage and access for up to 100 patients

5.1.1.1 The system must support concurrent database access for 200 users

5.1.2 The system must take no more than five seconds for loading and updating time

5.1.3 The system must support data processing in no more than 20 seconds after a drive is completed to show accurate analysis of driving behaviors

5.2 Safety Requirements

5.2.1 The system must verify a patient's account before storing drive data

5.2.2 The system must disclose the usage of data and privacy policies

5.2.3 The system must obtain appropriate user permissions and use only information consented to

5.2.3 The system must provide a recovery method for data corruption

5.3 Security Requirements

5.3.1 The system must enforce unique accounts with robust passwords

5.3.2 The system must conduct user authentication and process data using JSON web tokens

5.3.2.1 The system must discern between physicians' and patients' accounts

5.3.2.2 The system must restrict the access of patients' data to their physician(s) exclusively

5.3.3 The system must collect only vital personal information about the patient

5.3.3.1 The system must anonymize all identifying information belonging to patients

5.3.4 The system must use AES 256 encryption for data migration to ensure data privacy

5.3.5 The system must allow for the deletion of any and all data pertaining to a patient during all stages

5.4 Software Quality Attributes

5.4.1 The system must be accessible on Android and iOS platforms

5.4.1.2 The system must be responsive on all devices

5.4.3 The system must accurately fetch and store data

5.4.4 The system must be accommodating in design for ease of patients' and physicians' use

5.5 Business Rules

5.5.1 The system must obtain sensor data from users' systems unobtrusively

5.5.2 The system must comply to the Health Insurance Portability and Accountability Act (HIPAA)

5.5.3 The system must provide different processed driving data for physicians and patients

6. Legal and Ethical Considerations

6.1 Data Privacy

A core aspect of our application is the collection of information pertaining to an individual's driving habits. This includes raw data from sensors such as accelerometers and gyroscopes to measure an individual's drive times, acceleration habits, and angular velocities in addition to the individual's GPS data to record frequented routes—all of which have correlations with the severity of glaucoma. While data collected from the smartphone sensors are not personally identifiable information (PII), the GPS data stream is extremely sensitive, revealing the individual's frequented and current locations.

Given the risk associated with GPS data leakage, the application takes many measures to secure the data. Primarily, the software used for data collection, data transmission, and data storage is from reputable and secure organizations with built-in encryption systems. Additionally, selling the user's data is prohibited. Such measures ensure that the collected data is secure and not likely to leak.

In the event that data does leak during the data acquisition, transmission, and storage stages, the users shall not be identified as their identities are double-encrypted. That is, their user IDs are solely available to the physician and have no meaning during the data acquisition, transmission, and storage stages. If the data leak occurred on the physician's end, there is still no substantial damage, as the physician's view solely includes the list of user IDs belonging to their patients without keys mapping user ID to patient. The key is available solely through the physician's clinical records of the patient. Thus, for the user to be personally identified, the physician's clinical system must be compromised, which is not under the jurisdiction of this application.

6.2 California Consumer Privacy Act Compliance

In compliance with the California Consumer Privacy Act (CCPA), the user will be made aware of the data the application collects. The user may create an account only if they thoroughly read and agree to a statement of the data that will be collected from them. A checkbox will be placed next to every section of the statement to ensure that the user agrees to the statement. Additionally, a two-minute timer will be displayed for every section, during which the user is expected to read the section of the statement. The user will be unable to click the checkbox until the timer has expired. If the user does not agree to the data collection statement, they will be unable to create an account. They shall also have the opportunity to describe what aspects of the statement they were uncomfortable agreeing to.

Additionally, the user shall be able to access their personal data, which is solely composed of their age and GPS information. Raw sensor data will be available as well—in compliance with the CCPA—but will be unintelligible without the calculated driving score, driving habits, and driving events, which are solely available to the user's physician. Finally, users may also ask to delete their data.

6.3 Unobtrusive

The application shall be active while the user is driving. However, the application should not pose any additional risks to users with distractions such as notifications or blinking icons to indicate that the application is running. The user will have been made aware of this fact while reading the data collection statement.

Additionally, no detailed information, such as the user's driving score, driving habits, and driving events, will be made available to the user. Otherwise, the user may alter their behavior into one suitable for healthy individuals, which may be a safety hazard if their visual field does not support such driving habits.

6.4 Verification of Physician Identity

To protect the patients, any individual who creates an account as a physician must verify their status as a healthcare provider. This will be done by cross-verification of the physician's license information with the state the physician practices in, the American Board of Medical Specialties, and the American Medical Association. The physician must also provide evidence of their relation to the patient as their primary care physician or optometrist. This will be enforced by requiring the user to search for their physician's account in the application's database and send a request to the physician. The physician must then accept the user's request on their end. The two-way verification system ensures that both the user and the physician confirm their doctor-patient relationship. Additionally, patients will be aware of the physician who has access to their driving scores.

This system ensures that only individuals who are truly Board-certified physicians create a physician account and protects the user by informing them of the individuals who have access to their data. Otherwise, any individual can create an account as a physician and monitor a patient's driving activity and location.

6.5 Aid to Physicians

The application will primarily serve as an aid to physicians, providing them with data and information critical to monitoring their patients' visual conditions that are otherwise difficult to acquire. Ultimately, the physician uses their training and experience to make decisions and interact with the patient. The system shall not replace physicians through direct interactions with the patient through tasks such as consistently informing the patient of their current visual state or

diagnosing the patient. The only exception to this rule is in emergencies—if the system detects that the patient will soon progress to an irreversible stage of glaucoma that considerably impacts their daily life, then it will alert the patient to seek care from their physician or to rush to the emergency room. These considerations ensure that the application does not replace physicians or cause additional and unintentional harm to the patient by providing dangerous advice.

6.6 Assessment of System Benefits and Risks

While there are many potential legal and ethical risks within the system, substantial measures have been taken to mitigate such risks. With potential risks tempered, the potential benefits of the application (e.g., helping patients identify and treat glaucoma early, monitoring the progression of glaucoma, and informing further scientific studies on the relationship between glaucoma and driving events, etc.) substantially outweigh the potential risks.

Appendix A: Glossary

Advanced Encryption Standard (AES) 256: Symmetric cipher that generates a 256-bit key to encrypt and decrypt data

California Consumer Privacy Act (CCPA): State law that grants consumers rights over personal information collected and requires businesses to inform consumers about the collection, use, and retention of their personal information

Damoov: Telematics infrastructure that provides a software development kit for processing smartphone-sensor-collected driving data and configuration to internal online data storage platform DataHub

DataHub: Damoov's online data storage platform that acts as the backend configuration for products using the Telematics software development kit

Digital Phenotyping: Moment-by-moment quantification of human phenotype using personal digital device data

Glaucoma: General term for a group of eye diseases that damage the optic nerve and leading cause of blindness for individuals over the age of 60

Gyroscope: Measuring device in smartphones that measures orientation and angular velocity

Health Insurance Portability and Accountability Act (HIPAA): Federal law requiring national standards to protect medical information from being disclosed without a patient's knowledge or consent

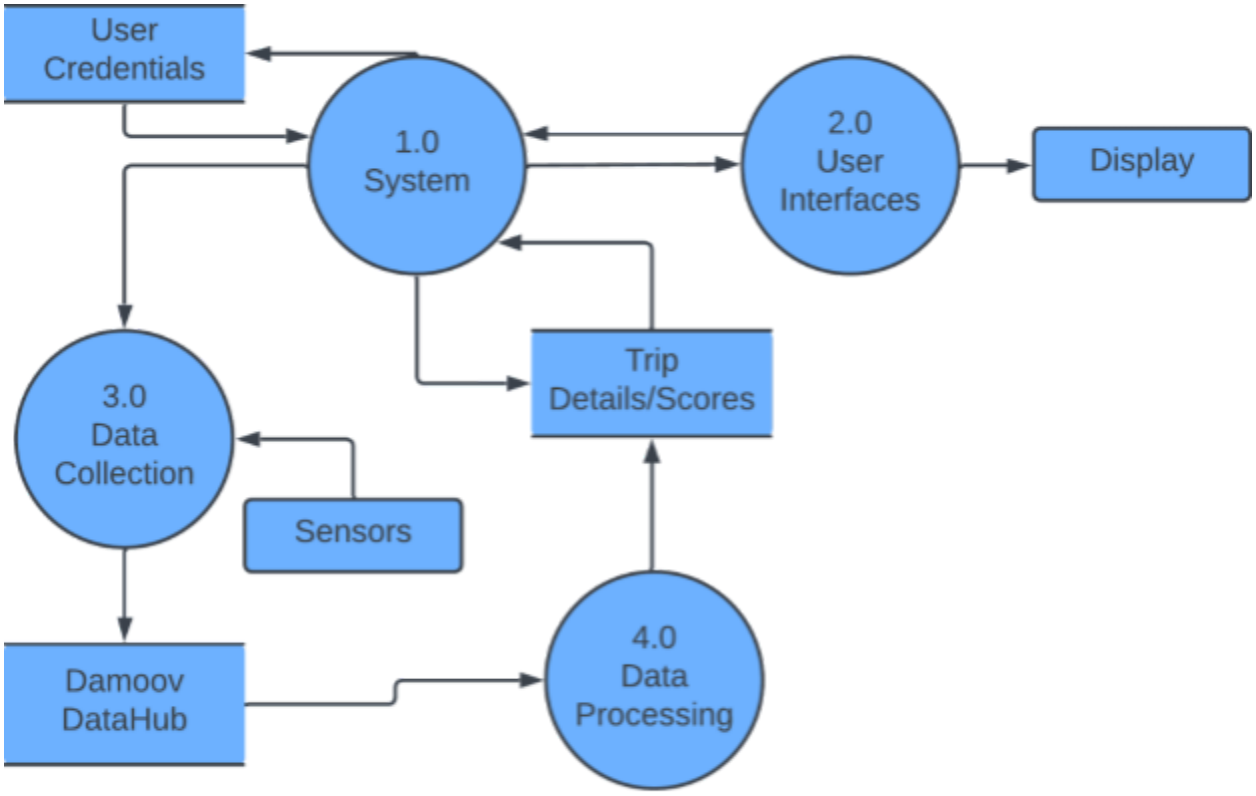
JavaScript Object Notation (JSON): Text-based, data-interchange format that can be structured as a list of a collection of name/value pairs or an ordered list of values

Magnetometer: Measuring device in smartphones that measures the magnetic field along using the axes of motion for orientation sensing

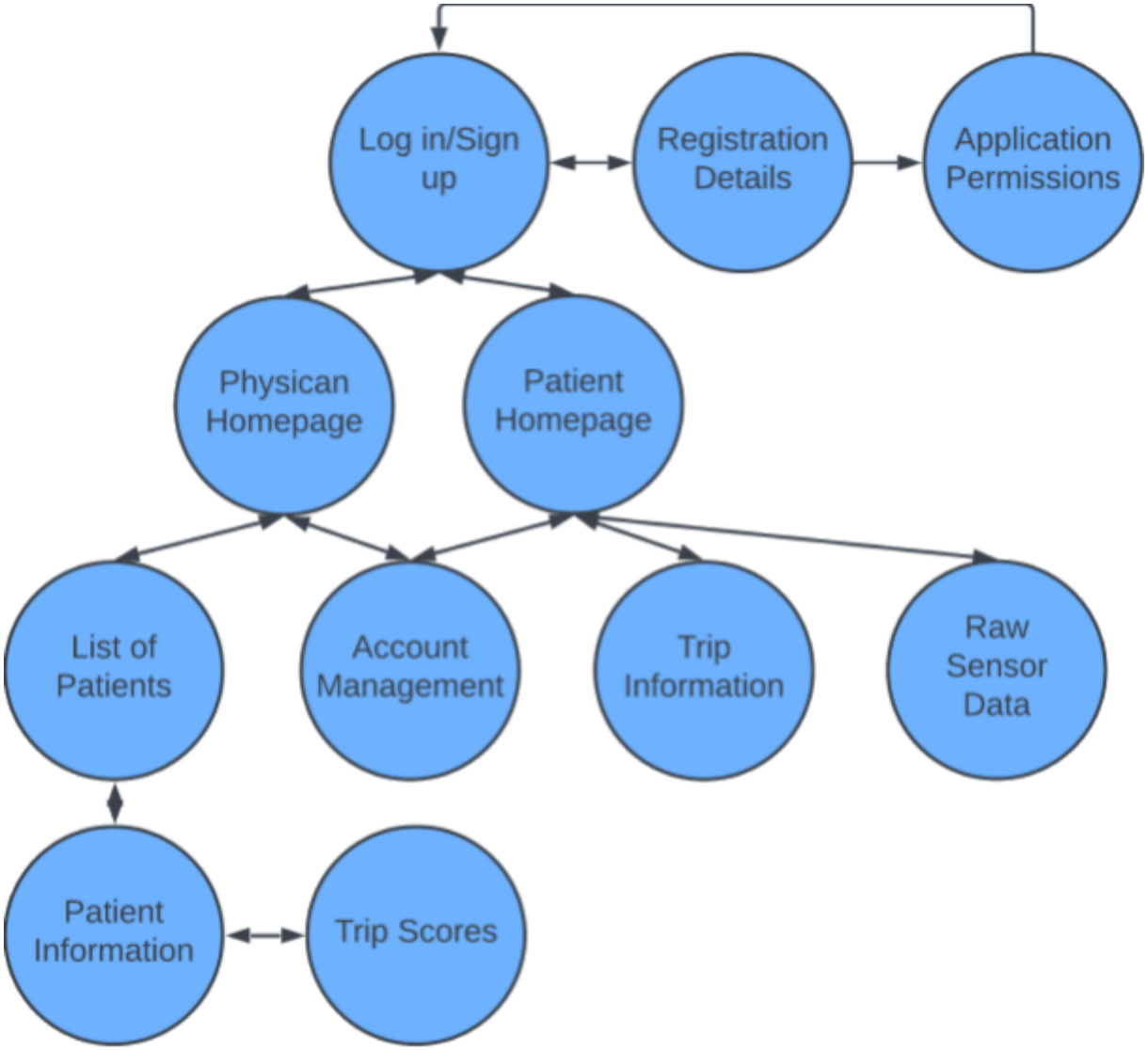
Triaxial Accelerometer: Measuring device in smartphones that measures acceleration using the axes of motion compared to gravity

Appendix B: Analysis Models

DFD Level 0



DFD Level 1



Entity-Relationship Diagram

Appendix C: To Be Determined List

None available at this time, as the application is still in the early development stage.