# **Requirements Document – Digital Medical Records – 3A04**

Why?

System Objectives:

- Safely store the medical information, so it can only be accessed by doctors and nurses.

- Implement an access control so appropriate information is given to the appropriate people.

- Allow authorized users to create, modify, and delete patient information.

- Store patient information including charts, records, and appointments.

- Generate reminders for patients to schedule appointments, and inform the doctor as well.

- Generate reminders to inform patients about upcoming appointments.

- Provide a visual plot of patient data (weight vs. height, weight vs. time, etc.)

- Allow for users to remotely schedule and cancel appointment dates. Notify the doctor about these appointments.

- Store the medical information in a way that is easily traversed by the user.

- Allow for medical staff to create their own personal username and password

Domain Knowledge:

-

-

-

-

Alternative Options:

- Could use an e-calendar in order to keep track of appointment dates.

- Have the choice of using a local database or server in order to store patient records.

- Could use a search engine to easily sift through patient records.

Conflicts:

-

-

What?

Functional Services:

- Information storage in a database.

- Encryption of information of database so it may only be accessed by those who are authorised.

- A user log in and authenticator (doctor, nurse, other) in order to grant specific permissions when viewing or editing patient data.

- Plots patient data, and displays it.

- Internal calendar which keeps track of upcoming and past appointments.

- Utilizing the internal calendar, reminds patients about upcoming appoints, and whether they are due for an appointment.

- Allows for authorised users to edit and delete patient data.

- Allow for patients to remotely cancel appointments.

- Keep patient records organised, and allow for easy traversal.

Assumptions:

- The users have remote access to the database.

- The users have web access in order to receive reminders.

- The users have a cell phone which can receive the given data.

- The users have a cell phone in which can run the given app.

Constraints:

- System has to store patient data somewhere

- System has to encrypt data so that patient records are private and secure

- System has to run on Android platform

- System has to have an authorization system that gives authorized users access to data that other users will not be able to see.

- System requires an internet connection to access app

- System must developed and completed by December 3, 2013

Who?

Users:

- Doctors

- Patients

- Nurses

- Interns

- Secretaries

Responsibilities:

- The medical staff is responsible for keeping the database up to date.

- The medical staff is responsible for keeping their login information private.

- The patient is responsible for picking a valid appointment date.

- The software-to-be is responsible for plotting the given data.

- The software-to-be is responsible for encrypting the data.

- The software-to-be is responsible for sorting and organising the patient records.

- The software-to-be is responsible for keeping an internal calendar.

- The software-to-be is responsible for generating and sending reminders to users.

- The software-to-be is responsible for keeping track of user log in information, and log in authentication.

- The medical staff is responsible for remembering their log in information.

- The hospital is required to provide a way to identify between the medical staff in order for the software-to-be to give the correct permissions to the database.

Functional Requirements:

Database:

- The system must have a database to store information.

- The database must be able to store text files as well as images, and must have a sufficient capacity

- The database must be accessible from multiple devices at the same time.

- The database must be able to accept new information, and updated patient records from devices.

- The system must encrypt data being saved to database to ensure patient records are kept private and classified.

- Database requires authentication to access

Authenticator:

- The system requires an authenticator to authenticate usernames and passwords.

- The authenticator must be able to decipher between multiple usernames and passwords.

- The authenticator must be able to appropriately award permissions to those who have been given them.

- The authenticator must request for the approved patient data after receiving the login information.

- The authenticator must be prepped with the correct username and passwords of those who are using the system

Encryption:

- The system must be secured through encryption, that means all passwords and patient data must be protected from all unauthorised sources.

Patient Data:

- The system must be able to store and display text and image files (Patient data).

- Patient data must be made to be editable by the user (updated, deleted).

- The user must be able to create new patient files.

- Patient height and weight must be organised in such a way that it is easily read, and can easily be plotted.

- System should remind patients of their upcoming appointments, as well as provide a record of previous appointments

Plotting:

- The user must be able to create simple charts and plots from patient data.

Calendar:

- The system must have an internal calendar which keeps track of upcoming and past patient appoints.

- The calendar must send notifications to the doctor/secretary/patient after a patient has gone an ‘x’ amount of time without an appointment.

- The secretary must be made aware of patients who have been sent notifications to book appointments.

Non-Functional Requirements:

- Patient files should be organised in alphabetical order, so it is easily traversable by users.

- Patient data must also be organised.

- The system must be made easy to learn and use.

- The system must respect doctor patient confidentiality and any other laws.

- System must have a graphical diagram showing patient data over time

- System must have a login feature to access app

- System must update user’s data to the latest data on the backend database

- System must hide detailed personal medical data from unauthorized users