Fortifying Healthcare.pdf

by Umajini Ravi

Submission date: 29-Aug-2025 03:24PM (UTC+1200)
Submission ID: 2737353739
File name: 182903_Umajini_Ravi_Fortifying_Healthcare_1734942_1181137795.pdf (1.42M)
Word count: 4503
Character count: 24378

Fortifying Healthcare

By Tech Power

Programme title	**Masters in Information Technology**
Course code and title	**ITPG8.600 Advanced mobile and wireless technologies**
Lecturer name	Mr Akbar Hossain
Assessment title	Assignment 02_Sprint 5
Due date	31/08/2025

PLAGIARISM DECLARATION

Plagiarism is a breach of EIT academic regulations. Penalties range from a warning to suspension or expulsion, as identified in the Student Handbook.

In signing this declaration, you acknowledge that you understand:

what constitutes plagiarism

that all work submitted for assessment may be screened for plagiarism

that this assessment will not be graded if it is found to contain any AI generated content, including output from generative tools such as ChatGPT, paraphrasing tools such as Grammarly, or other grammar checking tools

that any allegations of plagiarism will be handled according to the EIT Academic Integrity Procedure

I declare that the work submitted is my own work.

Name	ID	Signature	Date
Umajini Ravi	2025003781	*R.Umajini*	29/08/2025
Nabin K C	2025003724	*K.C.Nabin*	29/08/2025
S S E Jayantha Kumara	2025003875	*Jayantha*	29/08/2025
W M Sathya Paramie Wimalaweera	2025003692	*S.Paramie*	29/08/2025

Abstract

In Sprint 4, our efforts concentrated on translating user requirements into low-fidelity prototypes and user stories that captured real-world workflows for healthcare staff across multiple roles. This phase provided the initial structured visualization of the proposed mobile solution and established the foundation for subsequent refinements.

During Sprint 5, the focus shifted to advancing these preliminary designs into high-fidelity wireframes that reflected the detailed requirements derived from user stories. These wireframes incorporated refined user interface components, consistent design patterns, and realistic layouts, thereby providing a more accurate simulation of the final healthcare application. Enhanced fidelity improved the clarity of the prototype and ensured that the evolving system design aligned with usability, accessibility, and security requirements.

Building these wireframes, we developed and documented distinct user journeys, representing key roles within the system such as doctors, medical records officers, paramedic officers, and IT security staff.

By the conclusion of Sprint 5, we produced a realistic and functional prototype that accurately represents user workflows, strengthens security features, and establishes a robust.

Key Words: High-fidelity wireframe, user journey, healthcare application, secure navigation, system usability, Medical Record Officer (MRO)

Contents

1. Introduction

In the previous Sprint 4, we mentioned the user stories with low fidelity wireframes according to the four user groups who were addressing with main problem of the project. In this Sprint 5, we deliver the user journey and the high-fidelity wireframes for the main users who are going to use the mobile application. The user journey belongs to doctors, IT support staff, emergency report staff (Paramedic Officers), medical record officers, and common users.

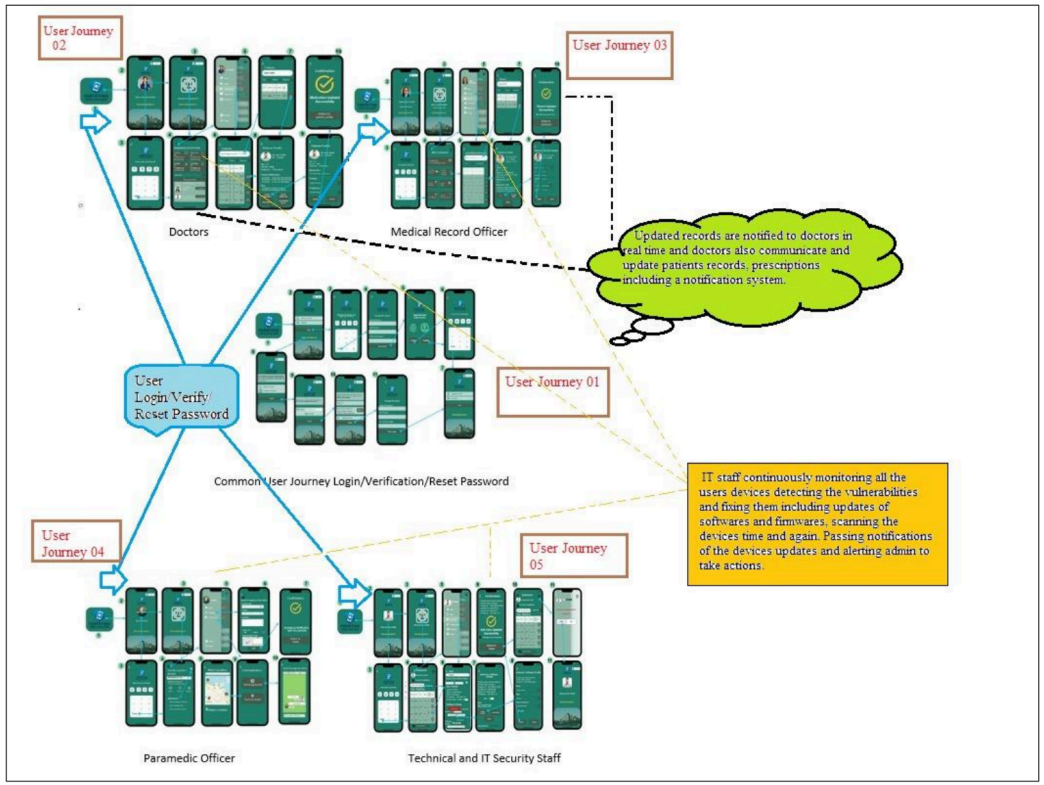

Figure 1 *Combined User Journey of Fortifying Healthcare (created using https://app.moqups.com)*

2. User Journey

1. User Journey 01

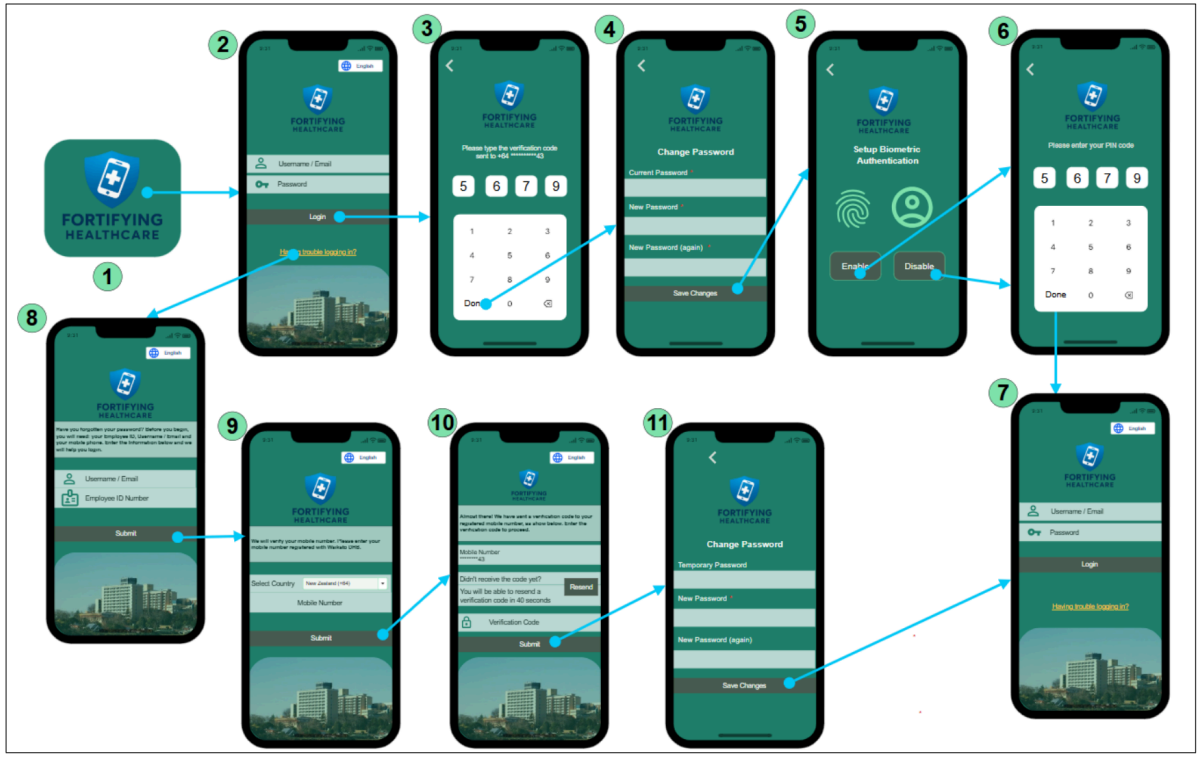

Figure 2 *User Journey 01 - Common Users [New or Existing] (created using https://app.moqups.com)*

1. The new user opens the application using an authorized device [No. - 01].
2. The user will navigate to the "**Login**" screen. [Screen no -02]. The application logo will display in the middle of the screen, and the "**Translation**" button will be displayed in the upper corner of the screen. From that user can change the language according to his/ her preference. There are two inputs to log in to the application,
    1) Username / Email – The user's valid Username or e-mail should be entered in this text field.
    2) Password – The user's valid password should be entered in this text field.
3. User taps on the **"Login"** button
    3) User will be moving to the verification screen [Screen no. - 03].
    4) User will be getting a verification code to the registered mobile number; he/ she need to enter the verification code in the "**Verification code**" input field.
4. User taps the **"Done"** button.
    5) The user will navigate to the "**Change Password**" screen [Screen no. - 04].
    6) In this screen, the user has to enter the temporary password as the current password and the new password in the **"New Password"** field.
5. Then, after the user taps on the **"Save Changes"** button.
    7) The user will navigate to the "**Setup Biometric Authentication**" screen [Screen no. – 05].
    8) In that screen user can enable or disable the biometric authentication.
6. The user taps any of the **"Enable"** or **"Disable"** buttons.
    9) The user will navigate to the setup PIN code screen [Screen no. 06].
    10) The user can use any 4 numbers to set up the PIN code.
7. The user taps on the **"Done"** button.
    11) After completing the authentication part, the user will automatically be taken to the login screen of the mobile application [Screen no. - 07].
    12) The user can use his/her Username / Email with the new password to log in to the "Fortifying Healthcare" application

When tapping on the "**Having trouble logging in?**" link [Screen no-02], the user navigates to [Screen no-8] to reset the password.

The "**Password Reset**" screen displayed a descriptive message like "Have you forgotten your password? Before you begin, you will need: your Employee ID, Username / Email, and your mobile phone. Enter the Information below, and we will help you log in."

There are two inputs in the "**Password Reset**" screen,

1. "**Username / Email**" input – To enter the valid username or email.
2. "**Employee ID**" input – To enter the valid Employee ID.

"**Submit**" button – To send the valid inputs to continue the password reset process.

After submitting, the user needs to enter the mobile number using the "**Verify Mobile number**" Screen [Screen no-9]. There are two inputs in this screen,

1. The user should select the country using the "Select Country" dropdown menu. After selecting the country, the country code will be selected in the "Select Country" dropdown.
2. "Mobile number" input – The user should enter a valid mobile number to continue the reset password process.
3. "Submit" button – To confirm the entered mobile number.

After submitting the mobile number, the user is navigated to enter the PIN code verification code confirming screen [Screen no 10]. This screen displayed the user-entered mobile number, and it displayed only the last numbers, to ensure privacy. There are two options to enter the PIN code to verify the login.

1. If the user didn't receive the "PIN code after 40 seconds," he/ she needs to tap on the "**Resend**" button to receive it again.
2. If the user gets the verification code, he/ she needs to enter the verification code in the "**Verification code**" input field.
3. "**Submit**" button – To continue the process of password reset.

After submitting the verification code successfully, the user will navigate to the last step of password reset, which is displayed in [Screen 11]. There are three user inputs displayed in this screen,

1. **“Temporary Password”** input – For security, ensure the user receives the temporary password via text message
2. **“New Password”** input – User should enter a new password in this user input.
3. **“New Password again”** input – User should enter the new password again in this user input.
4. **“Save Changes”** button – User needs to tap on this button to confirm the new password.

After saving the changes, the user will navigate to the “**Login**” screen [Screen no. - 07].

2. User Journey 02

User Journey – Doctor, viewing the patient's current medicine details, update the medicine and submitting to patients' data base.

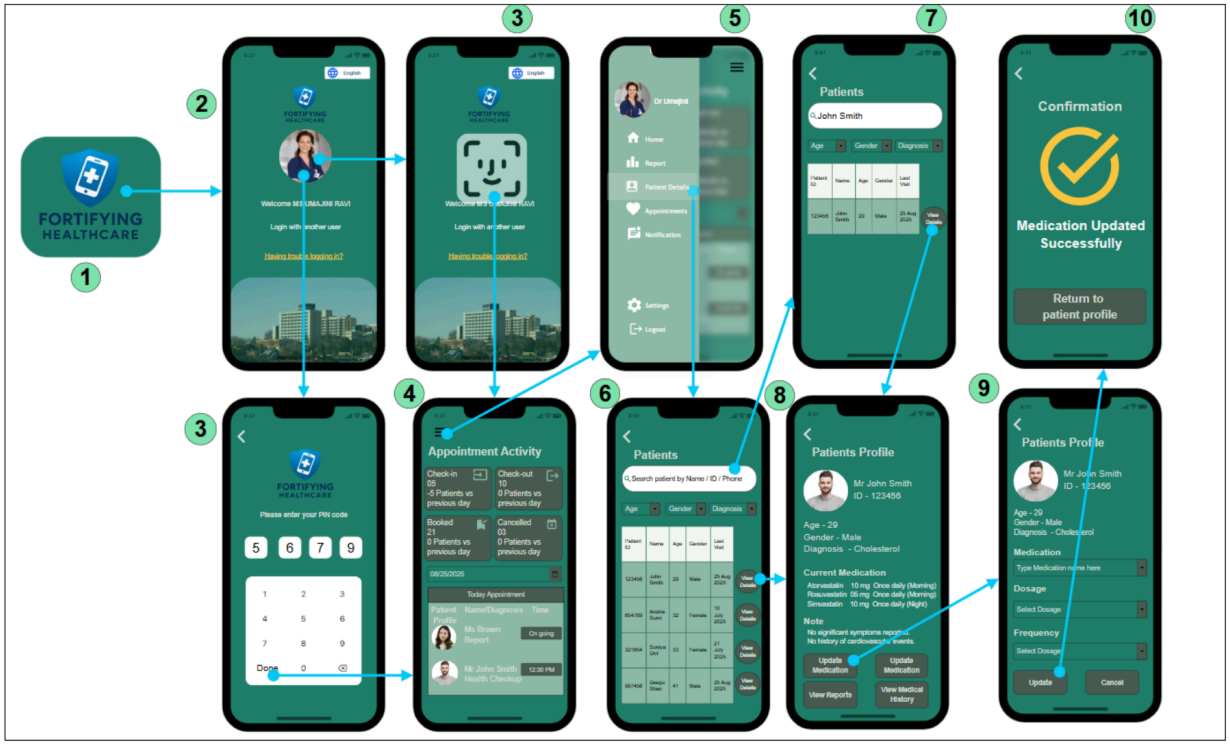

Figure 3 *User Journey 02 - Doctors (created using https://app.moqups.com)*

Doctors in hospitals and remote regions can safely access patient data by using the mobile application on approved devices. Through the app, they may simply change the patient's medicine depending on the reports and check the patient's medical history. The patient's records instantly update to reflect these changes. The user journey in the "Fortifying Healthcare" mobile app is described here, given a specific focus on how doctors update a patient's existing prescription.

1. The user starts the application on their authorized device.
2. If they are already logged in, their profile will appear on the login screen. The user then clicks **"User Profile"** [Screen no. - 02].
    1) User will be moving to two-factor verification screens, such as **"Bio Metric or PIN code"** screen [Screen no. - 03].
    2) If the login is successful, the user is taken to the doctor's dashboard, which includes appointment metrics and scheduled appointments. The user can change the date using the date picker to view past, present, or future appointments [Screen no. - 04].
    3) Also, the user can access more navigation choices using the **"Hamburger Menu".**
3. User clicks the **"Hamburger Menu"** [Screen no. - 04].
    4) The user's name and profile picture are shown at the top of the screen with quick access to the following sections of the mobile application [Screen no. - 05].
    5) **"Home"**: Takes user's home to the main dashboard, **"Reports"**: Provides access to patient reports, **"Patient Details":** Displays the patient search and patient details, **"Appointments":** Display the past, present and future appointments, **"Notifications"**: Shows system updates and messages from other staffs, **"Settings":** Updating preferences and user account settings and, **"Logout"**: A secure way to leave the application [Screen no. - 04].
4. User selects the **"Patient Details"** tile.
    6) The user will be taken to the next page, "Patient" dashboard [Screen no. - 06].
    7) On this dashboard, the user can search for patients using the **Search Bar** (by name, ID, or phone number) or filter results by age, gender, and diagnosis.
    8) If the patient was recently visited to the hospital, it's automatically shown in the patient details table on the dashboard [Screen no. - 06], or else if the user searched and got the patient details on it [Screen no. - 07].
    9) After all, the patient details will appear in the table.
5. User selects the **"View Details"** button.

10) User will land on the patient profile dashboard [Screen no. - 8].
11) The dashboard shows the patient's full details, including name, ID, age, gender, diagnosis, present drugs, and remarks.
12) At the bottom of the screen, there are four clickable buttons such as **"Update Medication":** Make changes to the patient's existing prescription information, **"Update Note":** Modify or add clinical notes to the note, **"View Medical History":** Examine the patient's past medical records and, **"View Record":** Access the whole patient record with the image of scan reports.

6. The user clicks the **"Update Medication"** button.
13) User will be taken to the next dashboard to update medication [Screen no. - 9].
14) The dashboard shows the patient's full details along with three selection panels such as **"Medication", "Dosage",** and **"Frequency**".
15) The user has to select the new medicine name, medication dosage, and medication taking frequency.
16) Bottom of the dashboard, there are 2 clickable buttons, such as **"Update"** and **"Cancel".**

7. The user clicks **the "Update"** button.
17) User will be getting a confirmation screen [Screen no. 10], showing the message **"Medication Updated Successfully"**
18) At the bottom, a **"Return to Patient Profile"** button is available to navigate back to the patient profile

3. User Journey 03

Figure 4 *User Journey 03 - Medical Report Officer (created using https://app.moqups.com)*

Medical Records Officers (MROs) can securely log into the hospital mobile application and manage patient information. Using the app, they can search for a patient and update records such as demographic details, diagnosis, and treatment notes. Once saved, the system instantly updates the patient's records. The report describes the user journey in the Fortifying Healthcare mobile app, emphasizing how the MRO updates the patient's medical record.

1. The user starts the application on their authorized device.
2. If they are already logged in, their profile will appear on the "Login" screen. The user then clicks **"User Profile"** [Screen no. - 02].
    1) User will be moving to two-factor verification screens, such as **"Bio Metric or PIN code"** screen [Screen no. - 03].
    2) If the login is successful, the user is taken to the "**Medical record officer's**" dashboard [MRO Dashboard], which includes Generate Reports, Search Medical Records, Update Records, Share Files, Notifications, and Pending Uploads. From tapping on the "**Search Medical Records**" tile, the user is able to find patients. [Screen no. - 04].
    3) Also, the user can access more navigation choices using the **"Hamburger Menu".**
3. User clicks the **"Hamburger Menu"** [Screen no. - 04].
    4) The user's name and profile picture are shown at the top of the screen with quick access to the following sections of the mobile application [Screen no. - 05].
    5) **"Home"**: Takes user's home to the main dashboard, **"Patient"**: Provides access to medical records, **"Reports":** Displays the medical reports, **"Share Records":** provides share medical records to doctors, and other system users, **"Notifications"**: Shows system updates and messages from other staffs, **"Settings":** Updating preferences and user account settings and, **"Logout"**: To secure way to leave the application.
4. User selects the **"Search Medical Records"** tile.
    6) The user will take to the next page, "**View Medical Records**" dashboard [Screen no. - 06].
    7) On this dashboard, the user can search for patients using the **Search Bar** (by name, ID) or filter results by date and department.

8) If the patient already has medical records, automatically shown in the patient's medical details table on the dashboard [Screen no. - 06], or else if the user searched and get the patient's medical details on it. [Screen no. - 07].
9) After all, the patient details will appear in the table.

5. User selects the **"View Details"** button.
   10) User will land on the patient profile dashboard [Screen no. - 8].
   11) The dashboard shows the patient's full details, including name, ID, age, gender, GP, admission date, Ward, department, bed, and diagnosis.
   12) At the bottom of the screen, there are four clickable buttons, such as **"Edit":** Make changes to the patient's existing medical information, **"Generate Report":** allow to generate medical reports with the existing medical report, **"Share":** share medical reports with other system users
6. The user clicks the **"Edit"** button.
   13) User will be taken to the next page to update the patient's medical record [Screen no. - 9].
   14) The dashboard shows editable fields, and the user can change details of the patient's medical record.
   15) Bottom of the dashboard, there are 2 clickable buttons, such as **"Update"** and **"Cancel".**
7. The user clicks the **"Update"** button.
   16) User will be getting a confirmation screen [Screen no. 10], showing the message **"Record Updated Successfully"** and notification has been updated.
   17) At the bottom, a **"Return to Dashboard"** button is available to navigate back to the patient profile.

4. User Journey 04

User Journey: Paramedic Officer shares real-time data, secure messaging to communicate, and shares live location with the hospital.

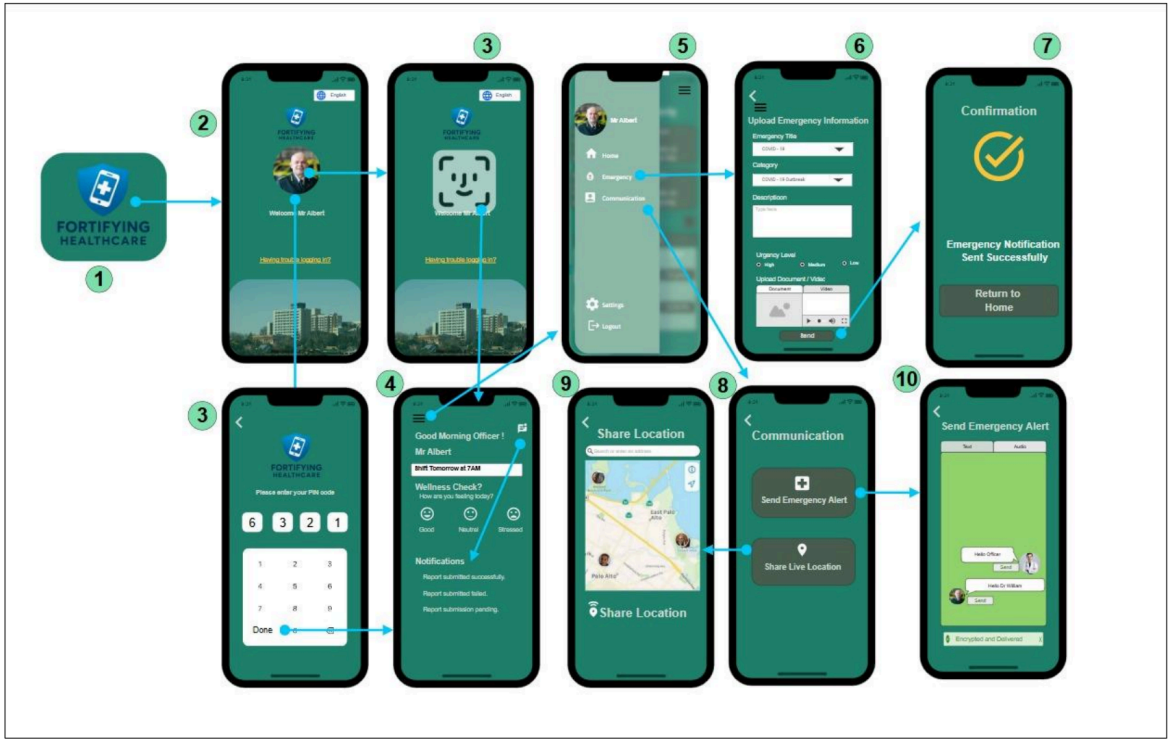

Figure 5 *User Journey 04 - Paramedic Officer (created using https://app.moqups.com)*

The Fortifying Health Care mobile application, which allows secured messaging for confidential discussion, real-time delivery of patient and emergency information needed by hospital systems, and a real-time GPS current place of residence tracker to assist with the hospital and disaster mitigation, is confidentially accessible only by licensed paramedic officers. The journey of a paramedic officer is mentioned below.

1. User launches the mobile application using an authorized device.
2. The user profile will display in the splash screen if the user has already logged in to the application. [Screen no-02]
    1) The user will navigate to the "**Two-factor Authentication**" screen, which includes entering the "**Bio Metric or PIN Code**" screen. [Screen no-03].
    2) If the login is successful, the user will navigate to the paramedic officer's "**Home**" screen, which includes a greeting, officers' coming shift details, feedback details, and notifications. [Screen no-04].
    3) The "**Hamburger Menu**" will navigate the paramedic officers' options in the application. [Screen no-04].
    4) The "**Notification**" button will notify how many notifications has received to the user and the bottom of the dashboard displays the notifications. [Screen no-04].
3. After the user taps on the "**Hamburger Menu**" [Screen no-04].
    5) The logged user profile details will display at the top of the navigation panel, and the officers' task is listed under the profile picture. [Screen no-05].
    6) "**Home**" option is navigated to the "**Home**" screen of the application, "**Emergency**" option is navigated to the screen to the screen, that enter the emergency details of the patient are entered. "**Communication**" option is navigated to the screen, to secure messaging with the doctor/ nurse. "**Settings**" option updates the user account settings, and "**Logout**" option is used to log out of the application.
4. When the user selects the "**Emergency**" option, the user will navigate to the "**Upload Emergency Information**" screen. [Screen no-06].
    7) On this screen [Screen no-06] user can enter the patient details and share them with the hospital. The user is able to select the type of emergency using the "**Emergency Title**" drop-down menu.
    8) The user can select the nature of the emergency using the "**Category**" drop-down menu.
    9) If the officer has any other notes, they can be entered in the "**Description**" box.

10) The user can select whether "**High**", "**Low**", or "**Medium**" radio buttons according to the urgency level of the patient.

11) Under the category of "**Upload Audio/ Video**," the user can select the "**Document**" or "**Video**" tab menus. From the selected type, the user can upload "**Documents**" or "**Videos**" of the patient.

12) After entering all the details, the user needs to tap on the "**Send**" button to communicate the details with the hospital.

13) After sending the details, the user will receive a success message "Emergency **Notification Sent Successfully**" in [Screen no-07], and when they tap on the "**Return to Home**" button, the user will navigate to the "**Dashboard**" of the mobile app.

5. When the user selects the "**Communication**" option, the user will navigate to the "**Communication**" screen. [Screen no-08]. There are two tiles displayed in the "**Communication**" screen,

14) "**Send Emergency Alert**" – it will navigate to the "**Send Emergency Alert**" screen [Screen no-10].

15) "**Share Live Location**" – it will navigate to the "**Send Emergency Alert**" screen [Screen no-09].

6. After the user selects the "**Send Emergency Alert**" tile, the user will navigate to the "**Send Emergency Alert**" screen [Screen no-10], and this screen also has a tab menu to select the type of alerts.

16) If the user selects, "**Text**" tab, the user can communicate with the doctor/ nurse using text messages.

17) If the user selects, "**Audio**" tab, the user can communicate with the doctor/ nurse using audio messages.

18) In both of the tabs, displayed "**Send**" button is displayed to send after typing/ recording the text/ audio.

19) After sending the audio/text, there displayed as "**Encrypted and Delivered**" to ensure the message is sent securely.

7. After the user selects the "**Send Live Location**" tile, the user will navigate to the "**Share Location**" screen [Screen no-09].

20) The user can search or enter the live location through the "**Search Bar,**" and the map will locate the searched or entered location. After that, the user will be able to tap on the "**Share Live Location**" button to communicate the real-time location with the hospital

User Journey 05

User Journey: IT Security Staffs, viewing and updating antivirus software on healthcare mobile application of staff and confirming the successful update of software notifying user via notification.

Figure 6 *User Journey 05 - IT Security Staffs (created using https://app.moqups.com)*

IT Security Staff can securely manage and configure system security on authorized devices using the Fortifying Healthcare mobile application. With this application, they first log in with multi-factor authentication (an optional feature of biometric login using face recognition on further log in), access their respective dashboard, view user statistics, scan devices, manage and update antivirus software, and firmware. IT Security Staff manage and monitor potential threats on users' devices with this application; however, one particularly effective user journey is shown, mentioning device antivirus update on the user device in real-time, including notifying the relevant user.

2

1. The user opens the application on their authorized device.
2. If the user is already signed in once from the device, their profile is displayed on the welcome screen, and they simply tap on the user picture as shown on (Screen no 2).
    1) Next, the system directs them to the "**Two-factor authentication**" screen, where they can verify identity through biometric recognition or a PIN code. (Screen no 3).
    2) Once the verification is successful, the application opens the main dashboard, which presents a table of user statistics such as User IDs, usernames, assigned roles, IP addresses, and activity status. At the top of the screen, the IT staff can refine results by typing into the search bar to locate a particular user or device.
    3) There is other information, like visibility of potential threats and scanning all devices at the bottom. (Screen no 4)
3. Additional navigation options are available through the "**Hamburger**" menu. The user taps the menu icon. At the top of the sidebar, the name and photo of IT staff are displayed, followed by the list of quick-access sections. (Screen no 5)
    4) **Home**: Returns the user to the main dashboard.
    5) **Alerts**: Shows system notifications and critical warnings.
    6) **User Details**: Provides a full profile of each registered user along with their device details and usage.
    7) **Manage Software**: Enables the management and updating of various software on users' devices.
    8) **Notifications**: Displays updates, reminders, and alerts in real-time.
    9) **Settings**: Allows adjustment of account and application preferences.
4. The IT officer selects the "**User Details**" option, then redirects to the "**User**" dashboard. (Screen no 6)

a. Here, the IT officer may also locate a user by entering a user ID or name into the search bar. If a device has already been registered, its information will appear directly in the user details table. The table displays:

10) User ID: User Input: [PH012(PH refers to pharmacy)]
11) Full Name: User Input: [Shanti Shahi]
12) Role: User Input: [Pharmacist]
13) IP Address: User Input: [192.168.1.12 (IP address of that device used by Shanti)]
14) Device Status: User Input: [Active] (Indicates the device is currently active. The IP officer can deactivate it by clicking a toggle button, which sends an approval request to deactivate the device in case of potential threats).

a. Beneath this section, details of the installed antivirus software on the device are shown with three action buttons below it, namely Change, Update, and Review. The IT officer clicks on the "**Update**" option just below the antivirus. There are also other software details and actions regarding it, such as firmware update and so on, with scrolling of the screen.

5. This action opens the "**Antivirus Software Details**" screen. (Screen no 7)

15) The screen provides complete product information, including:

- Product name: Norton Antivirus (Name of the antivirus installed on the device).
- Product Type: Premium
- Product ID: 12WE WE23 QW22(Old product ID)
- Installed On: 2024-09-09
- Expires On: 2025-09-09
- IP Address: 192.168.1.12
- An indicator showing the active status of the current software.
- Below is a note indicating the remaining days of software expiry and suggesting updating soon.
- At the bottom, several options are presented for the officer to take various actions, namely "**Update Software**", "**Scan Device**", and "**Reset**". There is a link at the end of the screen to view the legal information of the software.
- The IT officer selects the "**Update Software**" option.

6. The application then loads the Antivirus Software Profile Screen. (Screen no 8)

Here, the officer can edit or choose details:

16) Antivirus Name: Norton Antivirus (A dropdown button providing options of antivirus software)
17) Type: Premium (Choice of types of antiviruses in dropdown)
18) New Product ID: 12SE WE23 RS02 (new product ID purchased)
19) A check box to ensure the correct details.
    a. Two action buttons ("**Update**" and "**Cancel**") are displayed at the bottom. The IT officer chooses the "**Update"** button.

7. The system confirms the action by showing a success screen with details of the update and a message appearing as "**Antivirus Updated Successfully**". A notification is sent to the user in real-time regarding the software update. (Screen no 9)
8. The "**Return to Home**" button is displayed at the bottom of the page (Screen no 9) that redirects the user back to the dashboard. (Screen no 10)
9. Finally, the officer proceeds to log out of the system securely. A prompt appears asking: "Are you sure you want to log out?" with options as **Yes** or **No**. (Screen no 11)
10. By selecting **Yes**, the system ends the session and returns the IT officer to the Welcome Screen. (Screen no -12 or 2)

3. Conclusion

In Sprint 5, our primary focus was on transforming the initial low-fidelity designs into high-fidelity wireframes, enabling a more realistic and functional representation of the proposed mobile application. This sprint allowed us to visualize the final look and feel of the app while integrating detailed UI components and consistent design elements.

We successfully created five distinct user journeys, each supported by high-fidelity wireframes that demonstrate how different user roles interact with the system. These journeys highlight not only the screen-to-screen transitions but also the logical flow of actions required to complete key tasks, ensuring that the prototype reflects practical usability and clarity.

Through this sprint, we streamlined the user interface, applied design consistency, and began embedding more advanced navigation structures, which collectively provide a stronger foundation for future development and evaluation.

Sprint 6 will concentrate on designing and conducting a comprehensive usability testing plan. This will enable us to evaluate the effectiveness of the prototype with real users, identify potential usability issues, and validate whether the design supports efficient, secure, and intuitive interactions for all identified user types.

Fortifying Healthcare.pdf

ORIGINALITY REPORT

4%	2%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Eastern Institute of Technology Student Paper	3%
2	Submitted to University of Birmingham Student Paper	<1%
3	fastercapital.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		