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 2
Due date	10/08/2025

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

Detailed and precise problem definition with reputable references. Mobile strategy addresses the problem well, but the justification could be more directly linked to each problem area. Strong technical section with layered requirements and security considerations.

Include diagrams showing integration with existing systems. Expand on contingency planning, offline operation scenarios, and post-deployment monitoring.

Marks: 8.5/10

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	09/08/2025
Nabin K C	2025003724	K.C.Nabin	09/08/2025
S S E Jayantha Kumara	2025003875	Jayantha	09/08/2025
W M Sathya Paramie Wimalaweera	2025003692	S.Paramie	09/08/2025

Abstract

This report addresses the critical IT system weaknesses of the former Waikato District Health Board (DHB), now part of Health New Zealand, which were exposed during the 2021 ransomware attack. The incident interrupted access to patient records, diagnostics, and communication systems, forcing a reversion to manual processes that compromised service delivery. To overcome such risks and enhance operational resilience, the proposed solution is a secure, cloud-integrated mobile application supported by wireless and ad-hoc networking protocols. The mobile strategy focuses on improving data security through multi-factor authentication, role-based access, end-to-end encryption, and real-time breach alerts, while ensuring seamless offline operation. Core functionalities include secure patient record access, encrypted communication, multilingual support, and integration with Electronic Health Records via FHIR APIs. The technical framework includes Mobile Device Management and portable mesh networks for emergency backup. This solution is expected to reduce maintenance costs, improve patient and staff satisfaction, and ensure continuity of care, especially in rural settings, ultimately fortifying healthcare delivery against cyber threats and operational disruptions.

Keywords: Zero Trust Network Access (ZTNA), Web Application Firewall (WAF), Electronic Health Records (EHRs), Fast Health Interoperability Resources (FHIRs), Mobile Device Management

Table of Contents.

1. Introduction

During Sprint 1, we identified the IT infrastructure and operational issues of the former Waikato District Health Board (DHB), now a subsidiary of Health New Zealand. The main issue was a poor IT infrastructure that triggered the May 2021 ransomware cyberattack. Due to the cyber-attack, the organization had many disruptions as follows:

- Patient records, emails, and diagnostic capabilities forced hospitals to revert to paper records, endangering patients.
- Waikato DHB had several systems, such as Electronic Health Records (EHR), scheduling, diagnosis, and personnel management, which were all hosted on a local server with a lack of security compliance, which forced the systems to be compromised.

The above points describe the manual processes being employed in certain rural clinics, which undermined service quality due to the lack of redundant systems in place as a current approach.

In the current sprint, the proposed solution is to implement a wireless mobile application aiming to provide fast, reliable and most importantly, a secure health service which ensures strengthening mobile healthcare along with communication continuity and resilience during those incidents or disasters by switching to work with ad-hoc networking protocols.

2. Mobile Strategy

By implementing a proper mobile strategy that ensures solving this problem and points out more details about mobile strategies, we solve these core problems discussed above.

2.1 Business Results

The initial step in designing the mobile strategy is identifying the business results that will be affected by the proposed solution. The designed business mobile strategy's business results are as follows:

1. Improving data security reduces the risk of secure remote access and inherent system redundancies.
2. Enhancing access is feasible from any location and can operate remotely through a centralized cloud-based system.
3. Reducing the cost of IT maintenance prevents unexpected expenses.
4. Improving patient and staff satisfaction through fast service delivery and more accurate records.
5. Enhancing maintenance and future updating, without system failure, using the staging or production and live environments independently.

2.2 Mobile Tasks

This section discusses the mobile strategy development of the proposed mobile application. In advance, the key features/ functions of the mobile application are discussed in the table below.

Table 1 *Mobile Tasks*

#	Mobile Tasks	Description
1	Registration for the mobile application, Login and Logout from the application	There is a need to add secure authorized user access for the application.
2	Login Notifications / Push notifications	The user is able to verify his/her login to the application successfully/not.
3	Language settings	There are different types of nationalities living in New Zealand and propose two main languages for the application.
4	Two factor authentication enabling	The authorized staff should be able to authenticate with password/ biometric authentication/pin code, followed by OTP.
5	Patient records display in the application	This organization main target area is patients, and the admin staff can view the records of patients.
6	Share/Exchange data securely	The application data is confidential, and it should be exchanged or shared securely.
7	Secure messaging	The messages encrypted and transmitted over channels, and it is not in plaintext.
8	Role based access	The application should be accessed for the authorized endpoints and logins.
9	Offline support in limited connectivity zone	When the application is offline, the data should be stored in a secure and once the application is online, the data should be synced without any interruptions.
10	Google analytics	It will provide the user analytics such as user actions, device logged locations and time, etc.
11	Real-time data breach alerting	It is necessary to get immediate reactions against a cyber-attack.

2.3 Functional Patterns

Each functional patterns have special elements that will define how the application works, who the users of the application are, what technologies are applied, and how it is suitable for the healthcare sector. Below we mentioned the:

Mobile Operation

- Authenticate and manage
- Enhance authentication
- Restrict app features
- Offline data storage and secure sync
- Detect and alert on security incident

Mobile Collaboration

- Encrypted communication through secure channels

Mobile Commerce

- Secure access to patient data
- Encrypted exchange of confidential data

Mobile Marketing

- Notify users of login success
- Support multilingual interface (MUI)
- Track and analyse user behaviour

The image below explains how the mobile application will interact with the main system to retrieve data securely.

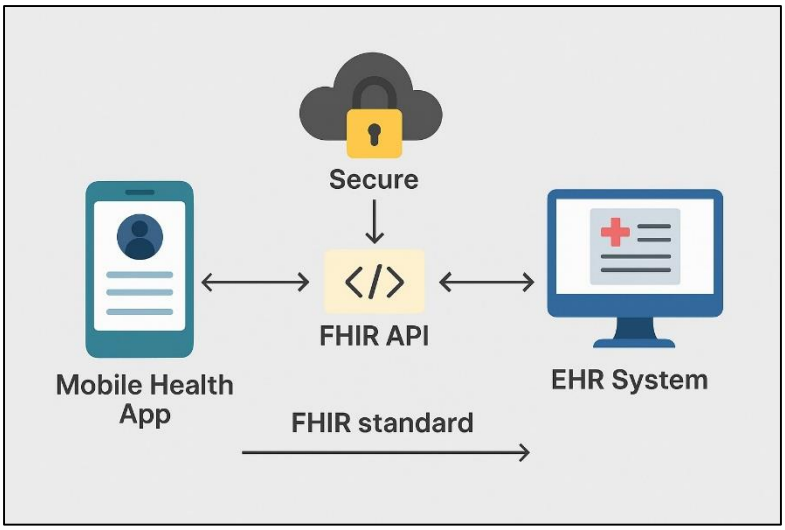

Figure 1 *Mobile application process overview*

3. Technical Requirements

Based on the overview of Waikato DHB and examining the sensitivity of healthcare, we came to the conclusion of developing a Native Mobile Application using both “Rich Client and Streaming Client” type Hosting. Below are the technical requirements for developing the mobile application regarding our mobile strategy;

Table 2 *Technical Requirements*

SN	Technical Requirements	Details
1.	User Interface Design	Simple, clean, user-friendly and accessible design with clear navigation and distinct functionalities.
2.	Security and Data Privacy	Application requires continuous identity verification (MFA, RBAC, OTP) for mobile users and IOT medical devices along with the use of Zero Trust Network Access (ZTNA) policies over mobile and wireless LANs, including secure communication protocols for data transfer (PFS, TLS and so on).
3.	Data Encryption and Secure API Integration	Application must have End-to-End Encryption (TLS 1.3 for all API calls and AES-256/XTS-AES for stored patients’ data) and API Gateway integrated with Web Application Firewall (WAF) to protect against DDoS or brute-force login attempts.
4.	Mobile Platform Support	Must run on both Android and IOS. Also, can integrate native modules for Android and IOS mesh functions.
5.	Mobile Device Management (MDM)	The application must implement an MDM system for devices/mobiles that access EHRs, along with restrictions for the installation of non-secure applications.
6.	System Integration	Compatible with Electronic Health Records (EHRs) sync via Fast Health Interoperability Resources (FHIRs) APIs for patients’ data exchange between devices and the central server.

7.	Emergency Backup System	Must have secure emergency backup communication via mesh network by the use of portable wireless mesh networks to create ad-hoc emergency backup communications among mobile devices and field hospitals with data synchronisation locally.
8.	Idle Timeout Detection and Session Handling	The application should store active session IDs, device ID, refresh token hash, role, IP, automatically sign out on idle timeout, along with clearing sensitive session data to avoid the risk of unauthorized access to sensitive information.
9.	Periodic Updates and Patching	Must have automatic security patch delivery via App Store/Play Store with secure CI/CD pipelines and security integration through the development lifecycle.
10.	Offline Access with Sync	Must provide offline notifications regarding appointment time remainder, previously synced records and sync securely with real-time data once back online.
11.	Database	Application stores data on a central server(cloud) deployed at Health New Zealand data centre, integrated with Couchbase Lite + Sync Gateway, which handles peer–to–peer sync and supports JSON documents (FHIR compatible).

4. Conclusion

In this report, we outline the core IT and operational vulnerabilities of the previous Waikato District Health Board, mainly the absence of resilient infrastructure that resulted in the 2021 ransomware attack. Our review pinpointed restricted remote access, ageing internal systems, and cybersecurity weaknesses. In response to these challenges, we recommended a mobile and wireless approach comprising cloud-based backups, mobile-enabled EHR systems, and secure remote access. The solution is anticipated to enhance data security, continuity of care, and access, particularly in rural regions. Adopting this approach will increase healthcare delivery and resilience throughout the Health New Zealand system.

The flowchart below explains the process before and after the implementation of the security mechanisms. This will be explained in detail in the upcoming sprints.

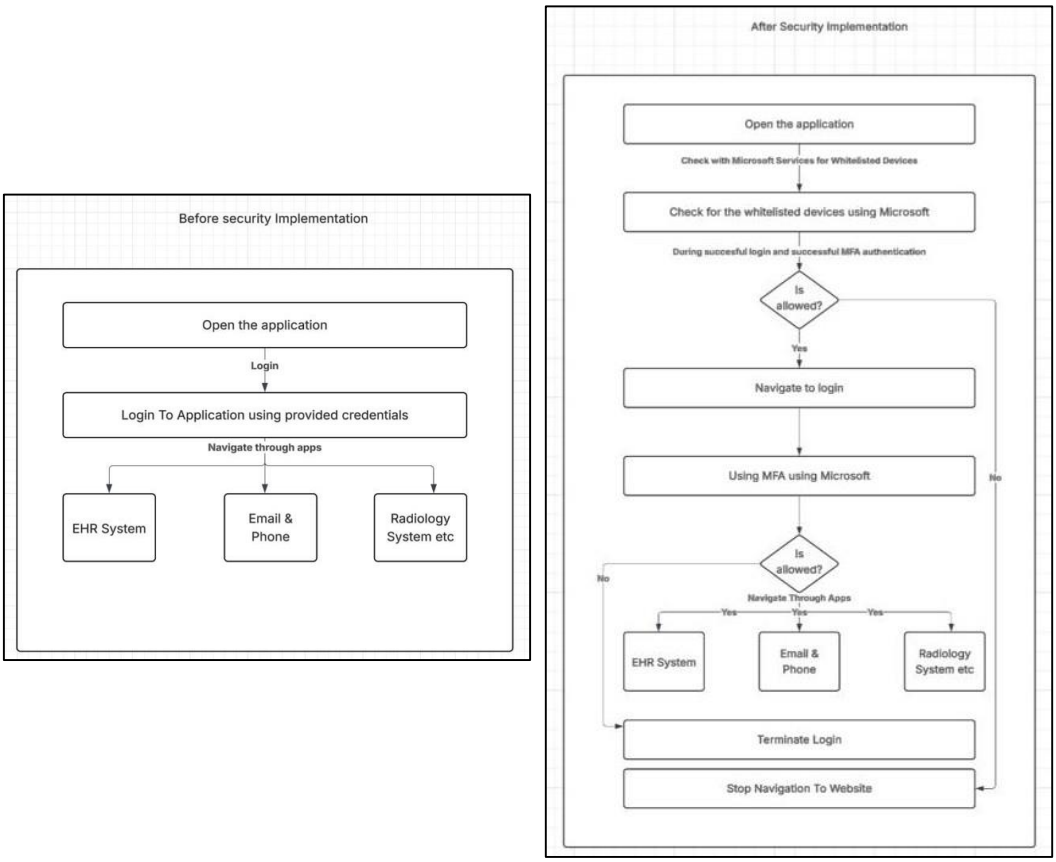

Figure 2 *Before and After Security Implementation (reference from ChatGPT)*

In the other hand, the following table chart explains the performance upgrade before and after the implementation of the security mechanism. This will be explained in detail in the upcoming sprints.

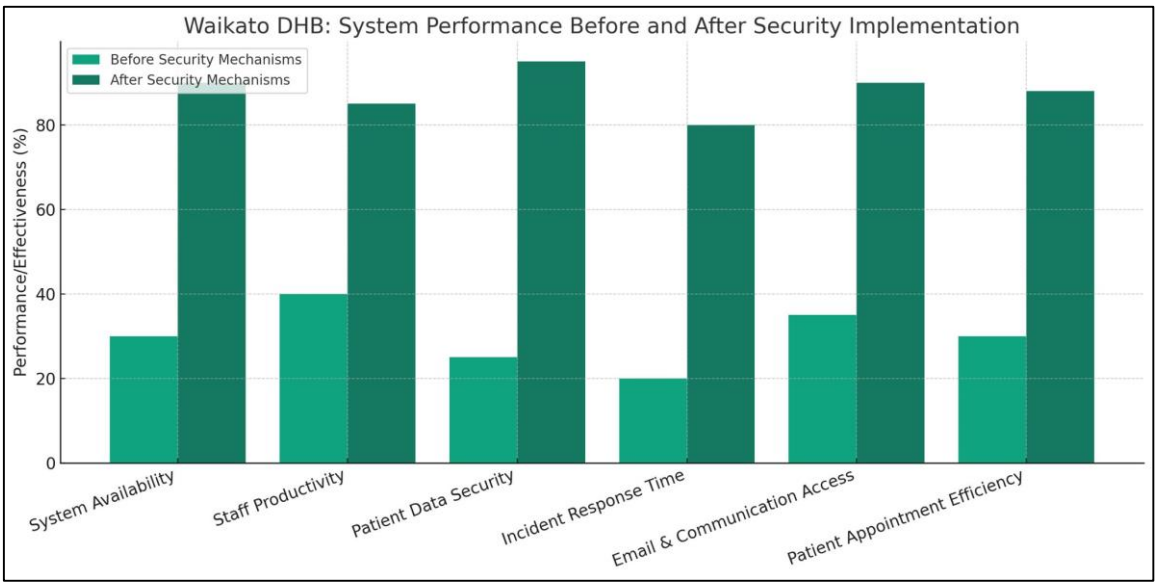

Figure 3 *Before and After performance (reference from ChatGPT)*

5. References

OpenAI. (2025). *ChatGPT* (4.1version) [Large language model] https://chatgpt.com/share/68971d58-b760-800c-9fff-a7dda38f6e01

OpenAI. (2025). *ChatGPT* (4.1version) [Large language model] https://chatgpt.com/s/m_6891ea96a43481919dc90a993ad197d2