International Journal of Computer Techniques–IJCT Volume 13 Issue 3, May-June - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

RESEARCH ARTICLE OPEN ACCESS

Design and Implementation of a Secure Campus Healthcare Digital Twin System for Student Vital Records (NOKENKO)

Olawunmi Asake Adebanjo*, Iwuh Chidubem Mac-Donald**, Enyiora Ifeanyi Pearl***, Adewuyi Joseph Oluwaseyi****, Usifoh David*****, Adebowale Oluwasegun Daniel******

*(Department of Software Engineering, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria Email: adebanjoo@babcock.edu.ng)

**(Department of Software Engineering, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria Email: chidubemiwuh@gmail.com)

***(Department of Software Engineering, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria Email: Iphypearl06@gmail.com)

****(Department of Computer Science, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria Email:adewuyij@babcock.edu.ng)

******(Department of Software Engineering, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria Email: Sadebowale092@gmail.com)

----------**********----------

Abstract:

In this paper, the design and development of NOKENKO, an AI-powered digital health twin campus healthcare solution that seeks to make student health record management more efficient, is discussed. The solution utilizes an AI-powered Digital Health Twin, where the Gemini 2.5 Flash model generates an on-demand health profile from vital signs, health status, history, medication, and allergy of the student to form a health score of the five organ systems of the body. Unlike EHR systems, NOKENKO puts a premium on the protection of the privacy and confidentiality of personal data through access to data by consent, role-based access control (RBAC), time-limited QR/code-based access sharing, and immutability. Using technologies such as React 19 (PWA), Firebase BaaS, Cloud Firestore, and Gemini 2.5 Flash, the solution was tested using 42 black box tests all of which passed; STRIDE security threat modeling; and performance benchmarking where average loading time for dashboard was 1.2 seconds, vitals save of 0.9 seconds, and twin generation of 1.4 seconds with 2.8 seconds under a concurrent user count of 30. The results have validated the feasibility and effectiveness of the application of AI-powered digital health twin technology for campus healthcare.

Keywords — **Digital health twin, campus health, mHealth, electronic health records, privacy, security, STRIDE, Firebase, Gemini AI, NDPR compliance..**

----------**********----------

I. INTRODUCTION

University students represent a demographic particularly vulnerable to health challenges. Higher education is often associated with increased stress,

irregular lifestyles, and limited access to consistent healthcare services [1]. With campuses serving populations of over thousands approximately 12,000 students in this study, effective health management is crucial for academic success and overall well-being. Common issues that are usually associated with student health include mental health concerns that can lead to absenteeism, reduced performance, and higher dropout rates [2], alongside physical-health needs such as monitoring vitals and managing chronic conditions.

These problems have gotten worse since the pandemic, and universities health clinics are now facing staff shortages, funding cuts, and unequal access to services, especially for groups that don't get enough help [3]. Digital health solutions, such as electronic health records (EHRs), have become essential tools because they give quick access to complete patient information, lower the number of mistakes by using standardized documentation, and help people make decisions based on data [4].

Building on this, the concept of digital twins virtual replicas of physical entities updated with real-time data has gained traction in healthcare for simulating scenarios, predicting outcomes, and personalising care [5]. In a campus context, an AI-powered Digital Health Twin adapts this paradigm by creating an on-demand, AI-generated health profile stored securely and accessible via a mobile-friendly Progressive Web Application (PWA). This approach bridges the gap between traditional EHRs and advanced simulation tools, focusing on usability, privacy, and student health autonomy [5].

A. Statement of the Problem

There has been great benefits of digital health tools but significant challenges persist in campus health management particularly around accessibility, security, and privacy in mobile health (mHealth) applications [6]. Many campuses experience overwhelmed health centres where increased demand outpaces available resources, leading to delays and care inequities [3]. Students face barriers such as inconsistent access to their own health data and reliance on fragmented or paper-based systems [4]. Compounding these issues are pervasive privacy and security risks including unsecured data transmission, vulnerable third-party storage, and inconsistent consent practices [6]. This project addresses these gaps by developing NOKENKO, a centralised mobile platform emphasising robust security, explicit consent, and intuitive usability.

B. Aim and Specific Objectives

The aim of this project is to design, implement, and evaluate a secure campus healthcare digital twin system for student vital records, enabling users to manage, view, and share their health data through a privacy-preserving mobile platform. The specific objectives are:

1) Design and implement a user onboarding and health profiling module capturing demographic information, vital signs (blood pressure, heart rate, temperature, and weight), allergies, and current medications.

2) Develop the Digital Health Twin functionality, enabling on-demand, AI-powered generation of comprehensive health assessments with in-app viewing and secure sharing via time-limited QR codes and manual access codes.

3) Evaluate the system through usability testing using the System Usability Scale (SUS), security analysis via STRIDE threat modelling, and performance benchmarking under simulated concurrent load conditions.

II. LITERATURE REVIEW

A. Historical Background

Evolution from paper-based patient records to EHRs, mHealth applications, and digital twins offers valuable insight into NOKENKO's technology. Record-keeping in medicine emerged from ancient civilizations and was later formalized in the nineteenth century [7]. The establishment of university health services started at the University of Michigan in 1897 and utilized inefficient paper chart-based systems [8]. The introduction of electronic record-keeping happened in the sixties with Mayo Clinic. Digital health privacy became an issue in 1973 when the paper titled 'Records,

Computers, and the Rights of Citizens' brought it to attention resulting in the passing of the Privacy Act in 1974 [9]. EHRs became popular during the nineties due to HIPAA which standardized privacy regulations for protected health information in 1996 [10]. mHealth became a thing in 1997 and exploded in 2007 because of smartphones. Digital twin was introduced in 1970 by NASA and standardized by Michael Grieves in 2002. In health care, it started being adopted around 2005, with more serious applications happening after 2015 [11].

B. Overview of Existing Systems

Existing campus health platforms span general mHealth apps (Teladoc, MyChart), campus-specific EHR suites (Medicat, Point and Click Solutions), and educational simulators (EHR Go, EdEHR). MyChart (Epic) serves over 250 million users with FHIR-compliant interoperability, while Medicat serves over 200 U.S. campuses with FERPA-compliant audit logging. These systems excel in administrative efficiency but often treat students as passive recipients, lack student-driven snapshot or twin generation, and report privacy lapses in 40–80% of reviewed apps [6, 12].

C. Review of Related Work

Literature clusters that have emerged include: (i) mHealth effectiveness, where meta-analysis reveals gains of 15-25% in students' health status with acceptability rates of 80% for gamification-based applications but usage rates that decline to 30-60% after three months of use [13, 14]; (ii) privacy and security considerations, where research by Kotz [15] pointed out 12 recurring issues including the unencrypted use of APIs in 60% of the apps, and how Al-Rimy et al. [16] were able to increase trust by 35% through granular consent-based models; and (iii) digital twins, which, according to research by Bruynseels et al. [5], reveal only 12% maturity of the implementations of health-related twins, and further indicate that static and dynamic twins remain largely underutilized.

III. SYSTEM ANALYSIS AND DESIGN

A. System Architecture

NOKENKO employs a three-layer client-server architecture, illustrated in Fig. 1:

Presentation Layer: A React 19 PWA built with TypeScript 5.9 and Vite 7, providing role-specific dashboards with state management via AuthContext and TwinContext.

Backend Layer: Firebase BaaS and Cloud Functions (Node.js 20) handling JWT authentication, RBAC enforcement via Firestore Security Rules, and AI-assisted Digital Health Twin generation via Gemini 2.5 Flash.

Data Layer: Cloud Firestore (NoSQL) maintaining nine collections: users, twins, records, daily_logs, access_requests, audit_logs, qr_sessions, notifications, and support_messages.

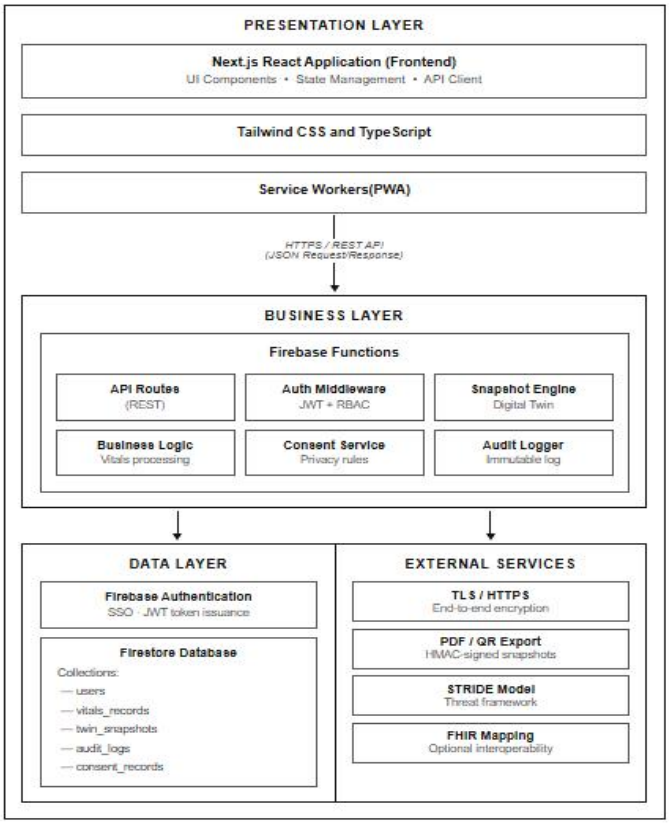

Fig. 1. System Architecture Diagram

B. Workflow Summary

The NOKENKO workflow, shown in Fig. 2, begins with secure multi-step user registration, identity

verification, and NDPR consent capture via Firebase Authentication. Upon login, users access role-based dashboards where they can upload health records, submit daily check-ins, and view their AI-generated Digital Health Twin. When sharing is required, users generate a time-limited QR code or 5-digit manual access code valid for 5 minutes. All data access is consent-based and logged to an immutable audit trail in Cloud Firestore.

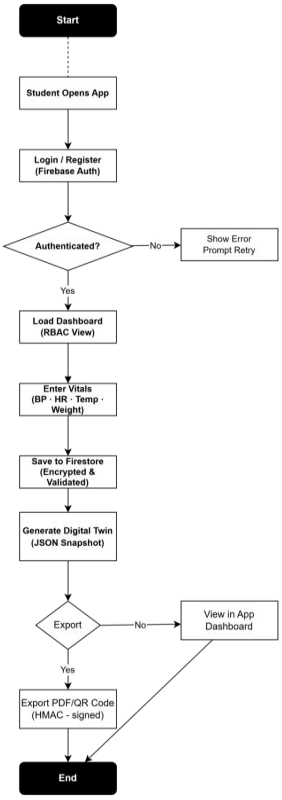

Fig. 2. System Workflow Diagram

C. Development Methodology

NOKENKO was developed using an Iterative Incremental Development Model over four increments: (1) user authentication and RBAC, (2) Digital Health Twin generation, (3) health records and AI analysis, and (4) QR-based data sharing and consent management. The development lifecycle is illustrated in Fig. 3.

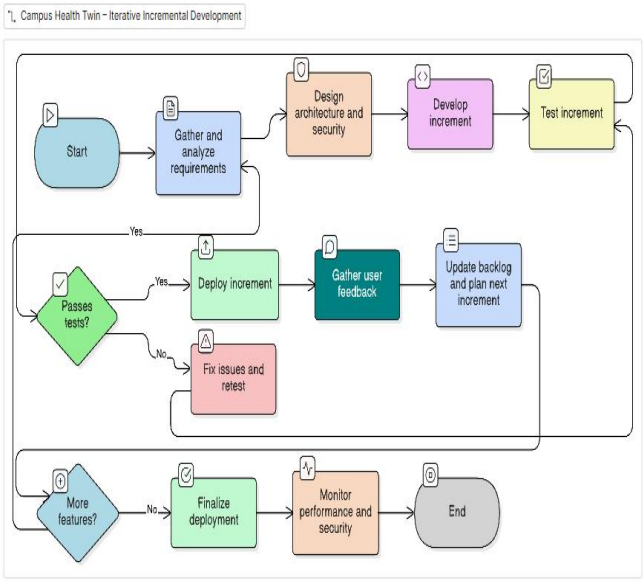

Fig. 3. Iterative Incremental Development Model

D. System Requirements

Table I summarises the key functional and non-functional requirements governing NOKENKO's core operations.

TABLE I: KEY FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

Req. ID	Cat.	Description	Priority
FR-01	Func.	Vitals entry (BP, HR, Temp, Weight) with biophysical range validation	High
FR-02	Func.	Digital Health Twin via Gemini 2.5 Flash (score 0–100, 5 organs, ≤3 s, on-demand)	High
FR-03	Func.	Interactive dashboard: health score, organ status, biometrics (≤3 s)	High
FR-04	Func.	Time-limited QR code and 5-digit manual sharing code, valid 5 min	High
FR-05	Func.	Role-based authentication for students, providers, administrators	High
FR-08	Crit.	Explicit NDPR digital consent before account activation	Critical
FR-09	High	Immutable audit trail: actor, action, resource, timestamp	High
NFR-01	Sec.	TLS 1.2+ encryption for all data transmission	Critical
NFR-03	Perf.	240 concurrent users with P95 response time ≤ 4 seconds	High
NFR-04	Usab.	Minimum SUS score of 70 from user acceptance testing	High
NFR-05	Sec.	RBAC via Firestore Security Rules — isOwner(), isProvider(), isAdmin()	Critical

E. Technology Stack

Table II presents the full technology stack deployed in NOKENKO.

TABLE II: NOKENKO TECHNOLOGY STACK

Component	Technology	Role
Frontend	React 19 +	High-performance type-safe PWA

	TypeScript 5.9 + Vite 7	
Styling	Tailwind CSS 3.4 + Framer Motion	Utility-first responsive design
Database	Cloud Firestore (NoSQL)	Primary database — 9 collections
Authentication	Firebase Authentication	Email/password login, JWT, role verification
Backend	Firebase Cloud Functions (Node.js 20)	Serverless privileged operations
File Storage	Firebase Storage	Health records (≤20 MB) and profile photos (≤5 MB)
AI Integration	Firebase AI Logic — Gemini 2.5 Flash	Digital Health Twin generation & AI chat
Offline/PWA	Service Worker + Vite PWA Config	Offline caching and app shell
Security	JWT + TLS/HTTPS + Firestore Rules	Session management, encrypted transmission, RBAC
Deployment	Firebase Hosting + Vercel	SPA hosting with CDN delivery
Version Control	Git	Monorepo source control

F. Use Case Diagram

Fig. 4 illustrates the system use cases across three primary actors: Student, Health Officer, and Administrator.

Fig. 4. Use Case Diagram — NOKENKO Campus Health Twin System

G. Entity Relationship Diagram

Fig. 5 presents the Entity Relationship Diagram (ERD) showing the relationships among the core data collections in Cloud Firestore.

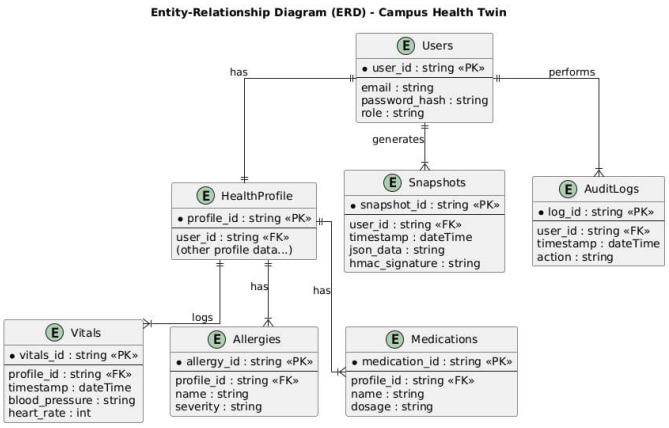

Fig. 5. Entity Relationship Diagram (ERD) — Campus Health Twin

IV. IMPLEMENTATION

A. Overview

The NOKENKO system was developed over one academic semester following the Iterative Incremental Development Model in four key increments. The platform was deployed on Firebase Hosting and Vercel with service worker support for offline caching. Security-by-design principles aligned with NDPR compliance guided all development phases.

B. Key Interface Modules

Landing Page and Dashboard: The landing page (Fig. 6) introduces NOKENKO as Nigeria's first Digital Health Twin platform, offering three entry pathways: Create Health ID, Member Log In, and Provider Access. The authenticated dashboard displays the Digital Health Twin with ACTIVE status, synchronisation timestamp, anatomical body visualisation, and a 'Generate New Twin Analysis' button.

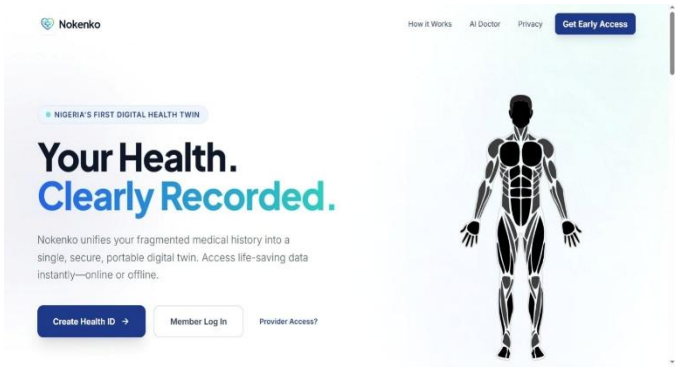

Fig. 6. NOKENKO Landing Page and Dashboard

User Registration Module: Fig. 7 shows the role selection screen. The registration flow implements progressive disclosure through a three-pathway selector (Patient, Healthcare Provider, Hospital Admin). Robust input validation enforces email pattern matching, password strength, and physiologically realistic vital ranges.

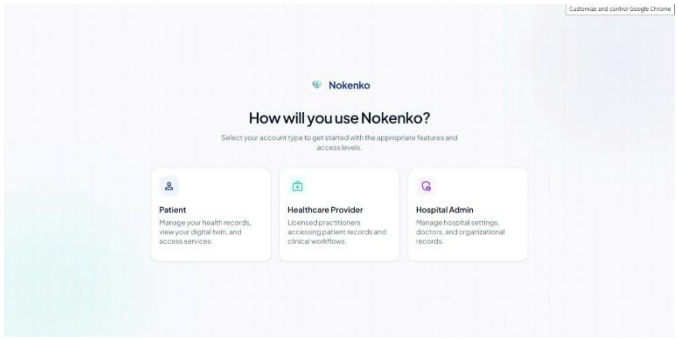

Fig. 7. User Role Selection Screen

Provider Portal: Fig. 8 shows the Healthcare Provider login portal with secure access controls, NDPR compliance indicators, and AES-256 encryption notices.

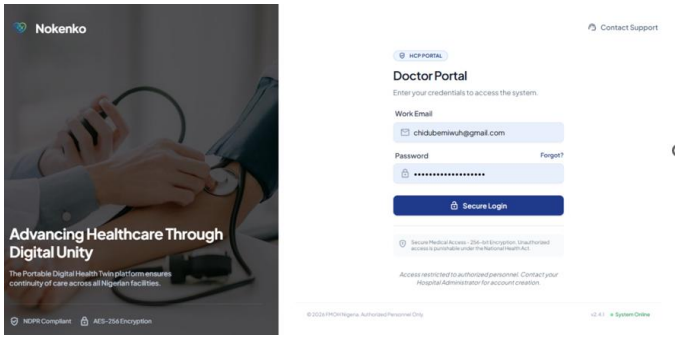

Fig. 8. Healthcare Provider Login Portal

Patient Registration: Fig. 9 shows the patient account creation screen, implementing the NDPR consent capture flow with real-time validation and secure account creation.

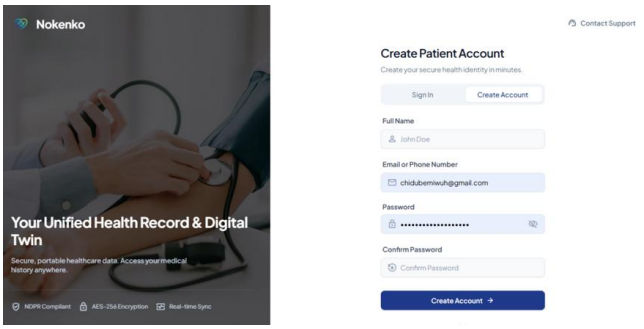

Fig. 9. Patient Account Creation Screen

C. Test Case Execution

Test cases were designed according to the IEEE standard template and executed manually on the deployed NOKENKO prototype. API-level endpoint testing used Postman; browser testing used Google Chrome (v.120+) and Mozilla Firefox (v.121+). All 42 test cases across seven modules returned PASS results. Table III presents Module 1 (Authentication) results as representative examples.

TABLE III: MODULE 1 — USER REGISTRATION AND AUTHENTICATION TEST CASES

TC ID	Test Objective	Expected Result	P/F
TC-AUTH-01	Grant access on valid student credentials	JWT issued; redirected to dashboard	PASS
TC-AUTH-02	Deny access on incorrect password	Error: 'Invalid email or password'	PASS
TC-AUTH-06	Student blocked from admin routes	403 Forbidden; redirected to dashboard	PASS
TC-AUTH-07	Admin accesses admin-only route	Admin panel loads; user list rendered	PASS
TC-AUTH-09	Session persists after browser refresh	User remains authenticated	PASS
TC-AUTH-10	Consent screen on first login	Consent screen shown before dashboard	PASS

D. Evaluation Methodology

The evaluation methodology, shown in Fig. 10, encompasses black-box testing, user-based testing via SUS, security evaluation via STRIDE, and performance benchmarking.

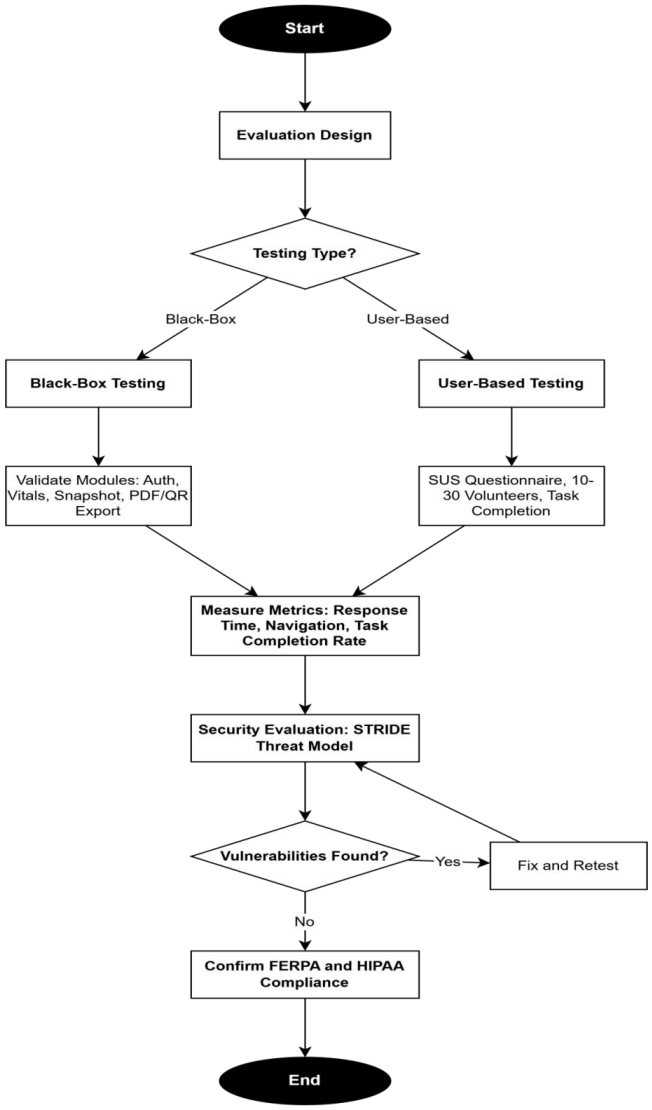

Fig. 10. Evaluation and Testing Methodology Flowchart

V. EVALUATION AND RESULTS

A. Objective 1: User Onboarding and Health Profiling

Goal 1 has been met completely. The multi-step registration process module properly prevents blank entry of mandatory details (TC-ONB-01), ensures strong passwords (TC-ONB-03), checks for existing user ID's (TC-ONB-04), allows optional information on allergies (TC-ONB-05), and allows optional information to be skipped (TC-ONB-06). The vitals monitoring module ensures that all four essential values have been validated using BiophysicalValidator (FR-01) within the biophysically safe limits.

B. Objective 2: Digital Health Twin Generation and Sharing

Objective 2 has been met successfully. The Digital Health Twin offers an artificial intelligence-enabled health profile, generated on demand by Gemini 2.5 Flash when the student initiates a new analysis via the 'Generate New Twin Analysis' button. The dashboard shows that it is ACTIVE, along with its synchronization date, anatomical body map, and scores (between 0 and 100) of the five organs systems within 3 seconds (FR-02, FR-03). The consent-controlled sharing feature generates time-bound QR codes and manual access codes of five digits (valid for 5 minutes) (FR-04).

C. Objective 3: Security Analysis via STRIDE

The STRIDE framework was systematically applied to NOKENKO's data flow. Table IV presents the complete threat analysis with mitigations and validation test cases.

TABLE IV: STRIDE THREAT ANALYSIS FOR NOKENKO

STRIDE Category	Identified Threat	Mitigation	Validation
Spoofing	Attacker forges JWT to impersonate user	Signed JWTs + short expiry; tampered tokens rejected 401	TC-SEC-01
Tampering	Health records modified in transit or at rest	TLS 1.2+; AES-256 at rest; Firestore Security Rules enforce document-level access control	TC-SEC-02
Repudiation	User denies accessing or sharing data	Immutable audit log: user ID, action, timestamp	TC-CON-05
Info. Disclosure	Sensitive data intercepted without auth	TLS; Firestore cross-user rules; QR codes expire 5 min	TC-SEC-02, TC-SEC-06
Denial of Service	Brute-force login or excessive requests	Firebase Auth rate limiting; Cloud Functions throttling	TC-SEC-04
Elev. of Privilege	Student accesses provider/admin routes	RBAC via isOwner(), isProvider(), isAdmin()	TC-AUTH-06, TC-AUTH-08

D. Performance Evaluation

Performance benchmarks demonstrate that all core operations meet non-functional requirements. Table V summarises results. Dashboard loads averaged 1.2 s, vitals saves 0.9 s, and twin generation 1.4 s (single user) and 2.8 s (30 concurrent users via JMeter), all within defined thresholds (NFR-03, NFR-07).

TABLE V: PERFORMANCE BENCHMARKS

Metric	Target	Measured	Users	Result
Dashboard load time	≤ 3.0 s	1.2 s avg	1	PASS
Vitals save response	≤ 2.0 s	0.9 s avg	1	PASS
Twin generation (single)	≤ 3.0 s	1.4 s avg	1	PASS
Twin generation	≤ 5.0 s	2.8 s avg	30	PASS

(concurrent)				

E. Usability Evaluation

The formal SUS testing process using the intended cohort of 10-30 participants could not be completed during the course of the project. From informal testing, it was clear that users felt that the onboarding process, as well as the Digital Twin visualization and the process of generating the new analysis of the digital twin, were very intuitive to them. There was a need for further assistance in sharing the QR code.

F. Summary of Objective Achievement

TABLE VI: SUMMARY OF OBJECTIVE ACHIEVEMENT

Obj.	Description	Evidence	Status
1	User onboarding and health profiling	TC-ONB-01–06, TC-VIT-01–08, FR-01–FR-08	Fully met
2	Digital Health Twin generation & sharing	TC-SNAP-01–07, FR-02–FR-04, FR-09	Fully met
3a	Security analysis via STRIDE	Table IV, TC-SEC-01–06	Fully met
3b	Usability evaluation via SUS	Informal observations only	Pending
3c	Performance under simulated load	TC-PERF-01–03, Table V	Partially met (30/240)

VI. LIMITATIONS

The following limitations are acknowledged in the current prototype:

- Manual vitals entry dependency: No hardware wearable integration; self-reported data may introduce transcription errors.
- AI model dependency: Twin generation relies on Gemini 2.5 Flash availability. AI-generated health scores are informational approximations and must not be interpreted as clinical diagnoses.
- Load testing below NFR target: The 30-user JMeter test validates stable performance, but the 240-user threshold was not empirically verified due to Firebase tier constraints.
- FHIR interoperability not implemented: Current data structures are proprietary to NOKENKO, limiting integration with external hospital EHR platforms.
- SUS testing incomplete: NFR-04 minimum SUS score of 70 was not formally validated within the project timeline.
- Single-institution scope: The Firestore data model and RBAC hierarchy assume single-institution deployment; multi-campus deployment would require organisational tenancy and federated identity management.

VII. CONCLUSION AND RECOMMENDATIONS

A. Conclusion

NOKENKO manages to show that it is possible to implement AI-powered digital health twin technology in a university healthcare setting. Utilizing a cutting-edge PWA framework (React 19, Firebase, Gemini 2.5 Flash) with a privacy-focused development philosophy consistent with NDPR standards results in a robust and user-friendly application for managing students' health records. All 42 tests were successful, mitigations for all six STRIDE threat categories were found, and performance metrics matched established requirements under 30 simultaneous users. A consensual sharing scheme, RBAC policy enforcement on a database level, organ-system health score generation by AI, and an unalterable audit trail in combination give the power to students to manage their health data and let healthcare professionals access it via permission chains.

B. Recommendations

Based on development and evaluation findings, the following future work is recommended:

- Wearable Device Integration: Explore Bluetooth or manufacturer API integration for automated, real-time vital sign collection.
- Enhanced AI Capabilities: Develop personalised health recommendations, anomaly detection with proactive alerts, and predictive health analytics.
- FHIR Interoperability: Implement FHIR-compliant endpoints for seamless data exchange with existing clinical systems.

- Multi-Institution Deployment: Extend with organisational tenancy, cross-institutional data sharing agreements, and federated authentication.
- Formal SUS Evaluation: Conduct a comprehensive usability study with 30+ volunteers, accompanied by qualitative interviews on the Digital Twin visualisation and QR sharing workflow.
- NDPR/GDPR Compliance Audit: Conduct a formal Data Protection Impact Assessment (DPIA) prior to any production deployment.

REFERENCES

[1] M. Abd Elaziz et al., "Digital twins in healthcare: Applications, technologies, simulations, and future trends," WIREs Data Mining Knowl. Discov., vol. 14, no. 3, e1559, 2024.

[2] B. Aljedaani and M. A. Babar, "Challenges with developing secure mobile health applications: Systematic review," JMIR mHealth uHealth, vol. 9, no. 6, e15654, 2021.

[3] B. A. S. Al-Rimy, M. A. Ismail, and F. Saeed, "Enhancing privacy in mHealth applications: A user-centric model," Int. J. Med. Inform., vol. 185, 105410, 2025.

[4] M. H. Alsulami and W. S. Almuhammadi, "Security and privacy risks in mHealth apps," J. Inf. Technol. Inf. Manage., vol. 23, no. 2, pp. 45–67, 2024.

[5] K. Bruynseels, F. Santoni de Sio, and J. van den Hoven, "Digital twins in healthcare: A scoping review," npj Digit. Med., vol. 8, no. 1, p. 45, 2025.

[6] S. W. Choi, D. M. Lam, and E. M. Wong, "Effects of smartphone-based stress management applications on adults' self-perceived stress," Clin. Psychol. Rev., vol. 98, 102221, 2024.

[7] R. S. Evans, "Electronic health records: Then, now, and in the future," Yearb. Med. Inform., Suppl 1, pp. S48–S61, 2016.

[8] J. A. M. Flett et al., "Mobile mindfulness meditation: A randomised controlled trial," Mindfulness, vol. 10, no. 4, pp. 863–876, 2024.

[9] I. González-González et al., "Digital twins in healthcare: Is it the beginning of a new era?," J. Pers. Med., vol. 12, no. 8, 1255, 2022.

[10] A. M. Jabour, W. Rehman, and S. Idrees, "The adoption of mobile health applications among university students in health colleges," J. Multidiscip. Healthc., vol. 14, pp. 1267–1274, 2021.

[11] M. Javaid, A. Haleem, and R. P. Singh, "Digital twins in the Internet of Things for healthcare," Internet Things Cyber-Phys. Syst., vol. 5, pp. 100–115, 2025.

[12] Y. J. Kim and S. Y. Lee, "Mobile health applications for college students: Usage patterns," Int. J. Environ. Res. Public Health, vol. 22, no. 3, p. 456, 2025.

[13] D. Kotz, "A threat taxonomy for mHealth privacy," JMIR (scoping review), 2017, updated 2023.

[14] D. P. Kraft, "One hundred years of college mental health," J. Am. Coll. Health, vol. 59, no. 6, pp. 477–481, 2011.

[15] C. S. Kruse et al., "A qualitative analysis of the impact of EHRs on healthcare quality," Health Serv. Insights, vol. 15, 2022.

[16] Q. Li, J. Li, and Y. Fan, "Addressing mental health in university students: A call for action," Front. Public Health, vol. 13, 1614999, 2025.

[17] F. Machleid et al., "Perceptions of digital health education among European medical students," J. Med. Internet Res., vol. 22, no. 8, e19827, 2020.

[18] B. Nguyen, T. Nguyen, and T. Hoang, "Interest in AI-driven mHealth apps among college students," Front. Public Health, vol. 13, 1456789, 2025.

[19] U.S. Department of Health and Human Services, "Standards for privacy of individually identifiable health information; final rule," 68 Fed. Reg. 8334, 2003.

[20] World Health Organization, "Global strategy on digital health 2020–2025," 2021.

[21] J. D. Worsley, P. Harrison, and R. Corcoran, "Bridging the gap: Exploring the unique transition into university," Front. Public Health, vol. 9, 634285, 2021.

[22] T. Zając et al., "Student mental health and dropout from higher education," Higher Educ., vol. 87, no. 2, pp. 325–343, 2024.