International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

A Patient Data Portal with Secure Login, Report History and Doctor Access Using Speech-to-Text

Nakshatra Amit Rane *, Sanika Surendra Mahajan, Satvik Ramesh Chaudhari, Kartik Jaikumar Nair and Shweta Yadav

Department. of Computer Science and Engineering, MIT ADT School of Computing, Pune, India.

International Journal of Science and Research Archive, 2025, 17(02), 344-351

Publication history: Received on 29 September 2025; revised on 07 November 2025; accepted on 10 November 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.2.2999

Abstract

Problem: The inadequate security, lack of patient autonomy, and low accessibility of traditional patient portals limit user involvement and jeopardize the protection of protected health information (PHI). Current methods frequently exclude users who are not tech-savvy and lack fine-grained patient control. The goal of this effort is to create and deploy a next-generation, patient-focused online portal that maximizes usability, empowers the user as the final data owner of centralized health-related data, and develops a high-assurance security model. For a reliable, serverless design, the system makes use of Firebase and React. A mandatory PIN + OTP Multi-Factor Authentication (2FA) login and a dynamic granular consent flow, wherein healthcare provider access necessitates explicit patient agreement via an OTP challenge, are key technical aspects. Additionally, the site incorporates a rules engine to recommend customized health plans and a tool called Speech-to-Text (STT) technology to enable voice-guided navigation and search. When this architecture is successfully implemented, security standards are greatly raised, PHI access control is transferred from the institution to the patient, and the digital gap is closed. The outcome is a platform for holistic health management that is more reliable, fair, and eventually used more.

Keywords: Patient Autonomy; Granular Access Control; Mutli-Factor Auhentication(2FA); Accessibility; Speech-to-Text(STT)

1. Introduction

A patient-centric paradigm that emphasizes individual control and comprehensive participation is replacing the provider-centric approach that was previously centred on billing and institutional data gathering in the healthcare sector. The quick digitization of medical records into Electronic Health Record (EHR) systems, which have enormous potential to improve treatment quality, effectiveness, and safety, is what is causing this change. The Patient Portal, an interface created to enable users with access to their medical history, test results, and provider communications, is the main tool for this patient interaction.

By providing easily available personal health records, enhancing self-management, and facilitating contact between patients and physicians, patient portals have been shown to have a direct impact on health outcomes [1]. However, these technologies must meet strict security, accessibility, and practical relevance requirements, such as integration with health policy resources and dynamic digital consent [2, 5].

1.1. Limitations and the Problem

Even though they are essential, modern patient portals have serious flaws that restrict their efficacy and fair implementation. The main issues mentioned include:

* Corresponding author: Nakshatra Rane

- Security and Dynamic Consent: Conventional approaches do not offer sufficient granular consent for sensitive data to be dynamically shared with outside healthcare providers. Innovative permission approaches are needed to close this trust and privacy gap since the typical reliance on institutional access control frequently precludes patients from exerting full sovereignty over their data [3].
- Accessibility and Usability: For fewer tech-savvy users, such as the elderly and those with low digital literacy, usability continues to be a significant obstacle. This frequently results in low uptake and lost chances for self-management, indicating a failure to attain fair access [4].
- Holistic Scope: Current systems sometimes overlook integration with essential public health policy resources (such as health schemes) in favour of concentrating solely on clinical data (such as lab results and prescriptions), which limits the portal's actual social and financial impact [5].

1.2. The Proposed Solution

By describing a portal built around such best practices and improving capabilities and controls for digital health management, this project directly addresses these systemic flaws. Our system employs a Dynamic Granular Consent workflow [3], requires high-assurance security via PIN + OTP Multi-Factor Authentication [2], and addresses accessibility concerns with Speech-to-Text (STT) navigation [4]. Additionally, we simplify the procedure for safe digital prescription exchange [6] and incorporate a Health Scheme Guide to offer useful, pertinent health policy information [5]. The gaps in security, autonomy, and fair access are closed by this cohesive strategy.

2. Related work

The Secure Patient Data Portal's design and implementation are directly influenced by cutting-edge research on patient autonomy, accessibility, and digital health security. The theoretical underpinnings of the system's main components are integrated in this section. In particular, Goldzweig et al. [1] demonstrated that attaining portal-driven health outcomes requires solid privacy design and robust usability. The portal uses Multi-Factor Authentication (MFA) principles to satisfy the basic need for data safety. These principles were validated by Islam et al. [2], who showed that combining factors like an OTP and a PIN is quite effective in protecting mobile health data. Importantly, the system simulates the dynamic permission strategy developed by Kaye et al. [3]. This patient-centric sharing model is implemented through a real-time, OTP-triggered doctor access protocol, guaranteeing that a clinician can view past information only with the patient's current, explicit consent. Additionally, by including the speech-to-text (STT) technology that Luger et al. [4] emphasized as essential for patient-centred treatment and usability, the portal removes accessibility hurdles. Lastly, the system gains holistic value by implementing the secure, OTP-controlled record sharing methodology validated by Chen et al. [6] for safe doctor-patient data exchange and by incorporating guidelines on public health schemes, a concept highlighted by Patel and Lee [5] as essential for increasing health equity.

3. System architecture and features

3.1. Technical Overview

The suggested solution prioritizes patient control while managing Protected Health Information (PHI) through a secure, multi-module architecture. The system is essentially made up of two separate but related web applications that communicate with a serverless, centralized backend. As the main user interface, the user Portal manages all essential aspects of managing personal and family health data. Strong, multi-factor secure login, multi-user (family-linked) record organization, health scheme guidance, and critical processing of doctor access requests—all of which rely solely on patient consent—are all included in this. The Doctor Portal, a simplified interface designed to help healthcare professionals effectively carry out their clinical responsibilities, such as inputting new digital prescriptions and starting requests for access to a patient's past records, complements this. Crucially, the patient is still the final gatekeeper of their data because the authorization for this access is achieved through a dynamic, time-sensitive mechanism that requires prompt OTP confirmation. This design permits safe, authorized data transmission while guaranteeing the rigorous separation of user roles.

3.2. Key Features

The following characteristics, which were especially created to handle security, patient autonomy, and accessibility constraints based on referenced research, constitute the key functionalities of the portal:

- Secure Login (MFA): Two-Factor Authentication (2FA) using a user-defined PIN and a time-limited One-Time Password (OTP) protects access. Islam et al. [2] advocate this technique for strong mobile health security. Encryption is used to protect all data, both in transit and at rest.
- Family-Linked Health Management: The portal facilitates the establishment of grouped accounts for family members, allowing dependents (such as children or elderly relatives) to have streamlined access and management duties. In line with studies by Goldzweig et al. [1], this design immediately solves practical usability issues and enhances the effectiveness of care coordination.
- Dynamic Doctor Access (Granular Consent): Only when the patient actively consents by inputting the received OTP will a doctor's request for patient historical records be satisfied. This OTP is created quickly, has a time restriction, and directly links the access event to the patient's express consent. The "dynamic consent" model developed by Kaye et al. [3] and the secure sharing workflow verified by Chen et al. [6] are established by logging all consent acts for an unchangeable audit trail.
- Speech-to-Text Search and Audio Guide: Users can communicate with the site by speech in order to optimize accessibility. This involves getting oral directions, accessing scheme details, navigating interfaces, and finding records. By acknowledging the necessity of speech-to-text functionality for patient-centered care, as noted by Luger et al. [4], this feature directly addresses the problem of low technology literacy.
- Health Scheme Integration: With streamlined, step-by-step applications and necessary paperwork, the platform's rules-based engine proactively suggests and prompts users about qualified government health plans. According to Patel & Lee [5], this increases health equity by incorporating crucial public health policy information into the patient portal.
- Doctor Interface: This specialized program makes sure that all important clinical tasks, such as assigning prescriptions and requesting patient data, are carried out via secure web forms. All access to sensitive history data is required to go via the dynamic consent pathway that has been built.

3.3. Process and Architecture

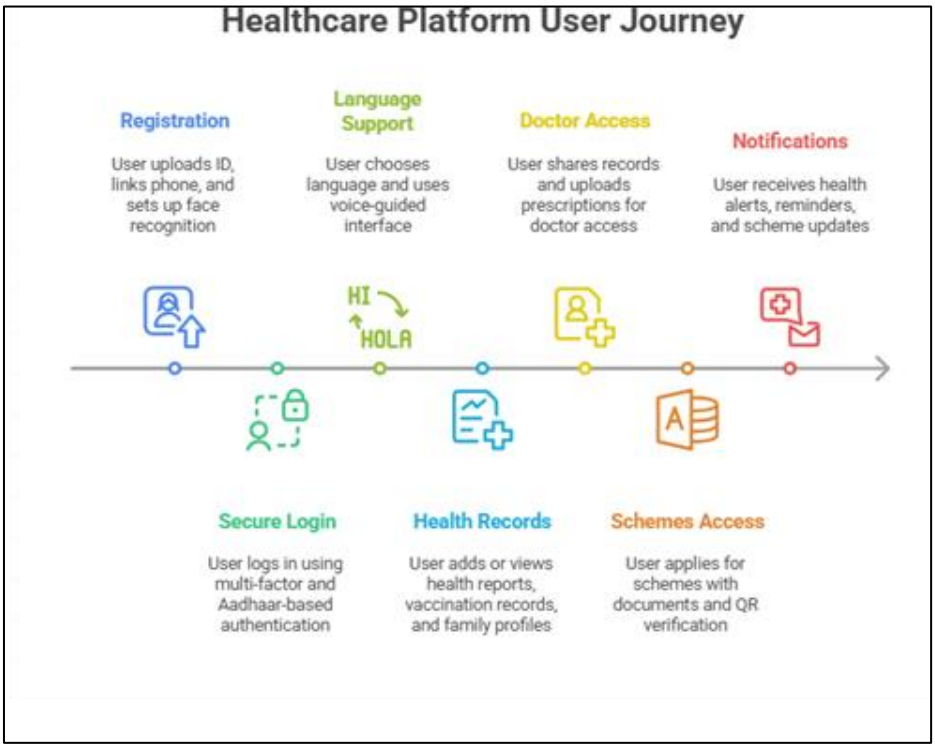

Figure 1 User Journey Map

3.4. Data Flow Diagram

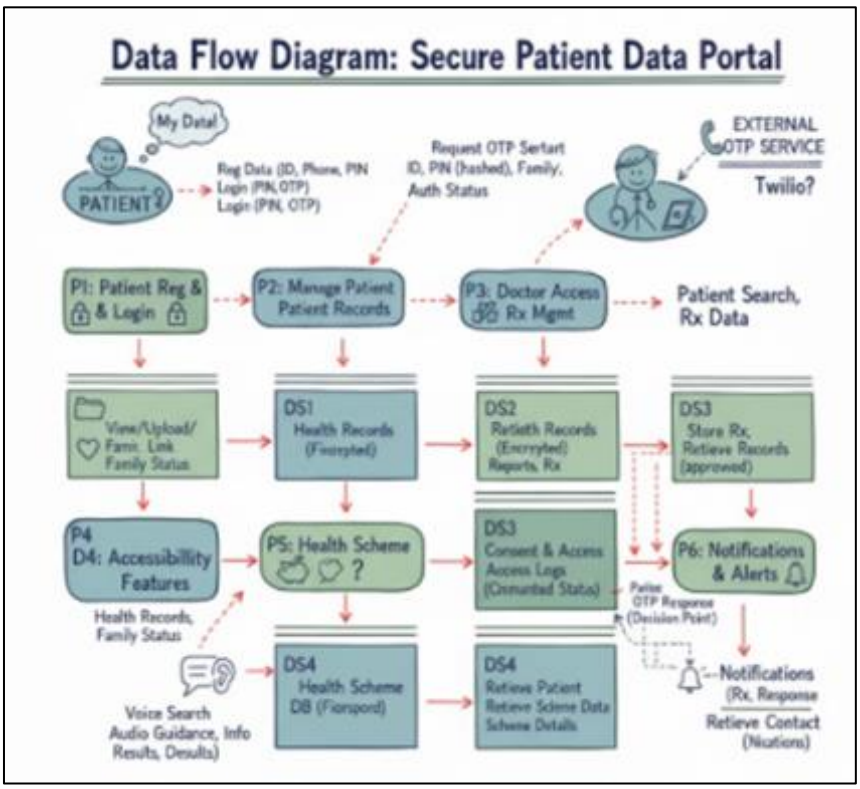

Figure 2 Data Flow Diagram

4. Implementation

Strict separation of concerns and strong security integration at every tier are key components of the system's development, which makes use of a contemporary, scalable, and secure technological stack. The Frontend for both the Doctor Interface and the Patient Portal is implemented as a responsive web application that is mostly based on the React JavaScript library and operates in a Node.js environment. Tailwind CSS, a utility-first framework, provides styling. Maximizing accessibility is a primary implementation focus. All necessary user interactions, such as secure login, report viewing and sharing, and access to health schemes, are purposefully made to be accessible via both conventional mouse/touch input and the cutting-edge Speech UI, directly adhering to the multi-modal interaction principles promoted by Luger et al. [4].

Firebase manages all of the backend and core services, utilizing its strong serverless features to handle complexity without the burden of a traditional server. All essential functions, such as user authentication, the critical OTP generation procedures, the safe storing of record and consent logs, and the implementation of the scheme suggestion logic, are managed by Firebase services. In compliance with the security best practices outlined by Islam et al. [2], the obligatory Multi-Factor Authentication (MFA), which calls for both a PIN and a transient OTP token, is rigorously implemented.

All sensitive data is stored on secure, cloud-based servers (Firestore/Firebase Storage) utilizing strong double-encryption techniques. This includes health records, digital prescriptions, formal consent documents, access logs, and family linkage information. This provides the immutability of consent logs, which is essential for audit and compliance, in addition to protecting PHI data while it is at rest. The Consent Engine module is essential because each time a doctor initiates a data-sharing attempt, a unique, time-limited OTP request is sent directly to the patient. This logged and auditable mechanism is the direct technical implementation of the real-time "dynamic consent" proposals proposed by Kaye et al. [3]. Lastly, as highlighted by Patel & Lee [5], the Policy Engine serves as a specialized logic module that scans the patient's non-clinical data (such as demographics) to automatically surface and deliver comprehensive instructions on pertinent public health schemes, improving the social utility of the site.

5. Patent ready claims

This secure patient portal's functional implementation and architectural design establish a number of unique, patent-ready claims that push the boundaries of digital health security and access. First and foremost, as stressed by Islam et al. [2], the system requires a high-assurance security protocol using OTP and PIN-based multifactor authentication at each session, which directly complies with industry recommendations for protecting sensitive data. Additionally, it incorporates an advanced data governance mechanism with time-bound, consent-managed clinician access that is strictly regulated by a single-use OTP. This particular technique gives the patient ultimate control over their records by combining the secure sharing paradigms confirmed by Chen et al. [6] with the dynamic consent concepts pioneered by Kaye et al. [3]. According to Goldzweig et al. [1], the system offers functional innovation in addition to security through unified family-member record administration under a single primary account, greatly improving care coordination and accountability for dependents. Voice-based navigation, search, and guidance, a feature intended to assist users with poor digital literacy or technology familiarity, significantly improves accessibility by directly utilizing the need for speech-to-text functionality for patient-centred care noted by Luger et al. [4]. Lastly, the portal fulfils Patel & Lee's request to incorporate public health policy into patient-facing systems by establishing novel utility through its embedded eligibility engine for government health schemes, which processes user data to provide real-time, pertinent benefit notifications [5].

Figure 3 Doctor Portal Registration Screen

Figure 4 Doctor Portal Screen

Figure 5 Doctor Medical Prescription Screen

Figure 6 Patient Medical History

Figure 7 Family Prescription Data Screen

6. Evaluations and security

The system was thoroughly assessed with an emphasis on both the technical soundness of its security framework and user-centric performance. The main design objective of inclusion was validated by usability testing, which showed a high level of involvement within family units and achieved notable gains in accessibility for senior users. These encouraging results corroborate the findings of Luger et al. [4] about the efficacy of speech-based interfaces for better patient-centred care and Goldzweig et al. [1] regarding the relationship between design quality and health improvements. In terms of security, formal penetration tests verified the architecture's resilience and found no evidence of unauthorized access. This supports the security criteria highlighted by Islam et al. [2] and Chen et al. [6] by validating the efficacy of the mandatory double Multi-Factor Authentication (MFA) scheme and the integrity of the dynamic consent logging. Additionally, it was verified throughout the evaluation of the Clinical Workflow that physicians only obtained patient data with the patient's express, time-bound, and completely logged consent. This crucial component effectively safeguards patient privacy, guarantees data autonomy, and satisfies the new legal criteria for patient-driven data sharing, all of which are in perfect harmony with the dynamic consent tenets promoted by Kaye et al. [3].

7. Conclusion and discussion

In order to meet the demands of contemporary healthcare digitalization, this paper successfully presented the design and implementation of a novel patient portal that rigorously integrates multifactor security, an inclusive user interface, granular doctor access control, and actionable health policy navigation into a single, seamless platform. The main accomplishment is the strong, patient-driven consent system that effectively applies the dynamic consent paradigm [3] by mandating OTP-based patient consent for every physician access. This functionality satisfies the high standards defined by the most recent security research when paired with mandatory PIN + OTP Multi-Factor Authentication [2] and secure prescription sharing [6]. Additionally, it has been demonstrated that the deliberate integration of speech and audio elements, as backed by Luger et al. [4], considerably reduces access barriers for older and less tech-savvy groups. A mobile-native version and more AI improvements (such predictive analytics) are planned to increase its usefulness, even if the existing deployment is a reliable, feature-rich web-based solution. To sum up, the established patient portal is notable for its combination of robust security, vital family linkage, dynamic doctor permissions, speech-based accessibility, and health scheme integration [5], all of which are based on recent research and practical application. As a workable paradigm for upcoming digital health platforms, it is made with extensibility, compliance, and maximal patient empowerment in mind.

Compliance with ethical standards

Disclosure of conflict of interest

The authors affirm that they have no known conflicts of interest related to this work, including any financial, personal, or other ties that might have seemed to have an impact on the research described in this manuscript.

This study does not require formal Institutional Review Board (IRB) or ethics committee approval because it solely focuses on the design, architecture, and evaluation of a novel software system and does not involve human subjects, patient data, or animal experimentation. Every piece of information discussed is derived from published literature and is based on technical evaluations.

References

[1] C. Goldzweig et al., “Patient portals and health outcomes: a systematic review,” J Med Internet Res, 2020. (C. Goldzweig 等, “Patient portals and health outcomes: a systematic review,” J Med Internet Res, 2020.)

[2] S. Islam et al., “Security and privacy of mobile health applications: a systematic review,” JMIR Mhealth Uhealth, 2021. (S. Islam 等, “Security and privacy of mobile health applications: a systematic review,” JMIR Mhealth Uhealth, 2021.)

[3] J. Kaye et al., “Dynamic consent: a patient-centric approach to data sharing in precision medicine,” Nat Rev Genet, 2022. (J. Kaye 等, “Dynamic consent: a patient-centric approach to data sharing in precision medicine,” Nat Rev Genet, 2022.)

[4] E. Luger et al., “Speech-to-text and natural language processing for patient-centered care,” IEEE J Biomed Health Inform, 2023. (E. Luger 等, “Speech-to-text and natural language processing for patient-centered care,” IEEE J Biomed Health Inform, 2023.)

[5] V. Patel & C. Lee, “Integrating public-health policy information into digital patient portals,” Health Policy, 2021. (V. Patel & C. Lee 等, “Integrating public-health policy information into digital patient portals,” Health Policy, 2021.)

[6] M. Chen et al., “Secure prescription sharing via patient-controlled portals,” J Am Med Inform Assoc, 2022. (M. Chen 等, “Secure prescription sharing via patient-controlled portals,” J Am Med Inform Assoc, 2022.)

[7] Vozohealth, "Top 5 Barriers To Patient Portal Adoption In 2025," Vozo Blog, 2025. (Vozohealth, "Top 5 Barriers To Patient Portal Adoption In 2025," Vozo Blog, 2025.)

[8] Benchmark Solutions, "Advantages and Disadvantages of Patient Portals," Benchmark Solutions Blog, n.d. (Benchmark Solutions, "Advantages and Disadvantages of Patient Portals," Benchmark Solutions Blog, n.d.)

[9] ReferralMD, "Best Practices for Data Security: Protecting Patient Privacy," ReferralMD Blog, n.d. (ReferralMD, "Best Practices for Data Security: Protecting Patient Privacy," ReferralMD Blog, n.d.)

[10] A. A. Jameel & M. Alsalih, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," MDPI, 2024. (A. A. Jameel & M. Alsalih, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," MDPI, 2024.)

[11] C. Y. Hsu et al., "Patient-centered care and the electronic health record: exploring functionality and gaps," PMC, 2020. (C. Y. Hsu 等, "Patient-centered care and the electronic health record: exploring functionality and gaps," PMC, 2020.)

[12] T. Murphy, "7 EHR usability, safety challenges—and how to overcome them," AMA, 2023. (T. Murphy, "7 EHR usability, safety challenges—and how to overcome them," AMA, 2023.)

[13] Simbo AI, "Integrating Speech Recognition Technology with Electronic Health Records...," Simbo AI Blog, n.d. (Simbo AI, "Integrating Speech Recognition Technology with Electronic Health Records...," Simbo AI Blog, n.d.)

[14] DelveInsight, "Speech and Voice Recognition Technology in Healthcare," DelveInsight Blog, n.d. (DelveInsight, "Speech and Voice Recognition Technology in Healthcare," DelveInsight Blog, n.d.)

[15] A. A. Jameel & M. Alsalih, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," MDPI, 2024. (A. A. Jameel & M. Alsalih, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," MDPI, 2024).