INTERNATIONAL JOURNAL OF PHARMACEUTICAL SCIENCES
[ISSN: 0975-4725; CODEN(USA): IJPS00]
Journal Homepage: https://www.ijpsjournal.com

OPEN ACCESS

Review Article

PharmaHealthia: One Stop Digital Solution for Patient and Healthcare

Rohan Kaswa*, Sakshi Kashid, Suyog Kamble, Aboli Kasar, Rutuja Kadam, Manisha Khaire

Rasiklal M. Dhariwal Institute of Pharmaceutical Education and Research, Late Dhodiba Detter Patil Marg, MIDC, Chinchwad, Pune, Maharashtra 411019

ARTICLE INFO

Published: 10 Feb 2026

Keywords:

Digital health platform; Integrated care ecosystem; Electronic health records (EHR) interoperability; Telehealth and remote monitoring; AI-driven clinical decision support; Patient engagement and self-management; Healthcare workflow automation; Health equity and digital inclusion

DOI:

10.5281/zenodo.18596929

ABSTRACT

In today's healthcare landscape, patients and providers face fragmentation: from multiple apps, disconnected records, and redundant workflows to constrained access, especially in remote or underserved areas [1,3]. PharmaHealthia is envisioned as a unified digital platform-bringing together patient, provider, pharmacy, diagnostics and wellness services under one roof-to streamline care, empower patients, and enhance clinical outcomes [3,5]. By integrating electronic health records (EHRs), tele consultation, medication management, remote monitoring, and analytics-driven decision support, PharmaHealthia addresses both the "front door" of patient access and the "back office" of provider workflows [2,3]. The platform fosters continuous engagement through personalized health journeys, reminders, patient education, and self management tools [1,5]. Simultaneously, it strengthens provider capabilities via real time data, interoperability, AI enabled insights and workflow automation [2,4]. Importantly, PharmaHealthia seeks to humanise digital health: the design emphasises intuitive user experience, empathy in patient provider interactions, trust, privacy and equity of access [1,2]. Implementation of such an ecosystem requires attention not only to technology, but to change management, usability, digital literacy, regulatory compliance and sustainable financing [2,5,6]. Early evidence from digital-health interventions shows promise in improving access, adherence, efficiency and outcomes-yet also highlights barriers around interoperability, usability, the digital divide and long-term integration into care pathways [1,3,4]. In that context, PharmaHealthia offers a holistic blueprint for a one stop digital health solution that aligns technological innovation with patient centred care, provider empowerment and system level transformation [2,3,5].

***Corresponding Author:** Rohan Kaswa

Address: *Rasiklal M. Dhariwal Institute of Pharmaceutical Education and Research, Late Dhodiba Detter Patil Marg, MIDC, Chinchwad, Pune, Maharashtra 411019*

Email ✉: kaswarohan02@gmail.com

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

INTRODUCTION

In many healthcare systems today, patients and clinicians alike navigate a fragmented landscape of disconnected apps, multiple portals, and siloed records. [7] The proliferation of digital-health technologies promises to link different components of care-such as diagnostics, pharmacies, remote monitoring, and patient engagement-into more coherent systems. [8] However, the mere presence of technology does not guarantee seamless integration, usability, or meaningful patient experience; design, workflow alignment and human-centredness remain major hurdles. [9] A fully integrated solution-one that brings together patient access, provider workflows, medication management and wellness services-therefore holds tremendous potential to streamline care, empower patients, and improve outcomes. [8,10] The concept of a "one-stop" digital ecosystem aligns with emerging research showing that digital health solutions can enhance healthcare access, especially in underserved or remote populations, while reducing administrative burden and redundancies. [7,10] Yet, to truly succeed, such a platform must go beyond feature-sets: it must humanise the experience, build trust, preserve privacy, support usability across populations including those with lower digital literacy, and embed itself into routine care pathways. [9,7] In this light, PharmaHealthia is proposed as a comprehensive digital-health architecture designed to unite patient-facing services, provider tools, pharmacy/medication modules, diagnostics, analytics and workflow automation-aligning technological innovation with the core value of patient-centred care. This review aims to examine the foundations, design principles, benefits, challenges and implementation considerations of PharmaHealthia, and situate it within the broader literature on digital-health transformation.

1.1. PURPOSE & SCOPE OF THE WEBSITE:

The website has been developed with the primary aim of securely managing patient health records while ensuring that access is tightly controlled and the potential for data misuse is minimised. By centralising patient information, including medical history, laboratory diagnostics, medication records, and treatment plans, the platform streamlines workflows for healthcare providers and administrative staff, allowing them to deliver care more efficiently and effectively. Patients, on the other hand, gain a transparent and reliable portal to access their own health information, empowering them to participate actively in their care journey. The platform is designed to cater to multiple user types, including patients seeking information and services, clinicians managing treatments, and administrative personnel overseeing operations, all while maintaining strict confidentiality. In an era where healthcare is increasingly digitised, the integrity and privacy of patient data are not just technical requirements but fundamental to building trust in the healthcare system. Ensuring that sensitive information is protected, and that patients feel secure in sharing their data, is central to both ethical healthcare delivery and the adoption of digital solutions. By prioritising these aspects, the website serves as a bridge between technological innovation and patient-centred care, fostering confidence among users while enhancing clinical and operational efficiency [11-13].

2. DATA MANAGEMENT ARCHITECTURE & WORKFLOW:

The data management architecture of the website has been designed to ensure a seamless, secure, and efficient flow of information across all user levels [14]. Patient data is entered into the system through authenticated portals, where it undergoes validation before being stored in encrypted databases that safeguard against unauthorised access or manipulation [15]. Each user-be it patient, healthcare provider, or administrator-has a predefined access level, determined by a role-based access control (RBAC) mechanism that ensures data confidentiality and minimises the risk of misuse [16]. The workflow begins when a patient or authorised healthcare professional logs in to the portal using a secure authentication system. Upon entry, users can perform specific actions such as uploading diagnostic reports, updating treatment information, or reviewing medical records [17]. The website's architecture follows a modular design, where individual modules like patient registration, clinical documentation, laboratory results, and pharmacy management communicate through secure APIs to maintain interoperability and data integrity [18]. All transactions within the platform are logged and timestamped, creating a transparent audit trail that tracks every modification, addition, or retrieval of data [19]. This traceability not only strengthens accountability but also enables early detection of any suspicious or unauthorised activities. Data is regularly backed up in secure cloud repositories, ensuring business continuity and resilience in case of system failures or cyber incidents [20]. To maintain data accuracy and consistency, the system implements automated error-checking algorithms and validation layers during data entry. These mechanisms help reduce duplication, eliminate inconsistencies, and ensure that medical information remains up-to-date and reliable for clinical decision-making [21]. The overall architecture is designed not only for secure storage but also for efficient retrieval-healthcare professionals can access patient information quickly, improving coordination and reducing administrative delays [15].

By combining interoperability, security, and usability, the data management workflow aligns with international standards for healthcare information systems. This ensures that the website is scalable, adaptable to regulatory frameworks, and capable of integrating with emerging technologies such as electronic health records (EHRs) and telehealth platforms. Collectively, these architectural principles support a system that is both technologically advanced and centred on patient trust and data stewardship.

3. SECURITY MEASURES AND PRIVACY CONTROLS:

In the digital era, data security and privacy are the foundation of trust between patients and healthcare providers [22]. The website is built upon a multi-layered security architecture that integrates encryption, authentication, and access control protocols to ensure that sensitive patient information remains protected throughout its lifecycle [23]. End-to-end encryption is applied both during data transmission and storage, preventing unauthorised interception or data breaches [24]. User authentication is enforced using multi-factor authentication (MFA), combining password protection with device-based verification or biometric identification, thereby ensuring that only verified individuals can access the system [25]. To minimise the risk of internal threats, role-based access control (RBAC) and session timeouts are employed, limiting users to data strictly relevant to their role and automatically logging out idle sessions [26]. The website adheres to Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) standards, ensuring global compliance with healthcare data protection norms [27]. These frameworks emphasize transparency, consent management, and the right of patients to access or delete their own data-a principle embedded into the platform's design [28]. Data handling policies ensure that every record modification is logged, and audit trails are maintained to detect unauthorised activities or suspicious access patterns in real time [29]. To further reinforce data integrity, the platform utilises blockchain-based verification and secure hashing techniques, making data tampering nearly impossible without detection [9]. Backup and recovery mechanisms are automated and stored on encrypted cloud servers distributed across multiple secure locations, ensuring resilience in case of system failures, ransomware attacks, or natural disasters [30]. Privacy by design is a core element of this system, meaning that every function-from login to data retrieval-is built with privacy considerations from the ground up [31]. Additionally, regular vulnerability assessments and penetration testing are conducted to identify security loopholes before they can be exploited [32]. Periodic training for administrative users and healthcare providers ensures continuous awareness of cybersecurity best practices, bridging the gap between technology and human responsibility [33]. Together, these measures create an ecosystem that prioritises trust, confidentiality, and accountability, aligning with the ethical standards of digital healthcare transformation and the growing demand for patient-centric data governance [22,27].

4. COMPLIANCE, ETHICAL & REGULATORY CONSIDERATIONS:

In the development of digital healthcare platforms, compliance with data protection and ethical frameworks forms the cornerstone of patient trust and system credibility [35]. The website has been meticulously designed to align with both national and international healthcare data regulations, ensuring that every element of data handling upholds legal and ethical standards. Within the Indian context, the platform complies with the Digital Personal Data Protection Act (DPDP) 2023 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which collectively safeguard the privacy and security of personal health information [36]. These regulations mandate obtaining explicit patient consent for data collection, defining retention periods, and ensuring secure storage, all of which are embedded into the platform's operational framework [37]. To maintain interoperability with global standards, the system also aligns with Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) requirements, particularly for users interacting from multiple jurisdictions [38]. This dual compliance ensures transparency in how patient data are used, transferred, and protected across borders [39]. Regular compliance audits and policy reviews are conducted to verify adherence to evolving healthcare laws and to mitigate any emerging risks associated with digital data handling [40]. Ethically, the website is grounded in principles of patient autonomy, transparency and informed consent, ensuring that users have full control over their data and understand how it will be used [41]. Patients can choose to share, restrict, or delete their records at any time, reinforcing their right to data sovereignty [42]. Transparent privacy policies and consent prompts written in accessible language help users make informed decisions, even if they have limited technical knowledge [43]. To promote equity of access, the platform incorporates features that cater to users with low digital literacy and those from underserved or rural regions [44]. The user interface has been simplified with local language options, voice-assisted navigation and visual cues that guide patients step-by-step through essential processes [45]. These design elements are intended to bridge the digital divide, preventing exclusion of vulnerable populations who may otherwise be left behind in the digital healthcare revolution [46]. Additionally, the website implements mechanisms to ensure algorithmic fairness and non-discrimination, preventing bias in health recommendations or access prioritisation [47]. Data anonymisation and de-identification techniques are used when information is shared for research or analytics, maintaining confidentiality while enabling innovation [48]. Through this multidimensional approach-balancing legal compliance, ethical responsibility, and inclusivity-the platform not only meets regulatory obligations but also fosters trust, accountability, and equity in digital healthcare delivery [35,38,41].

5. USABILITY, USER-EXPERIENCE & HUMANISATION:

In modern healthcare platforms, user experience (UX) plays a decisive role in ensuring technology adoption by both patients and healthcare professionals [49]. The website has been designed with a human-centred approach, prioritising simplicity, accessibility, and inclusivity to ensure that users from diverse backgrounds can navigate it with ease [50]. Each interface component-from dashboards to appointment modules-is developed to provide intuitive navigation and clear data visualization, reducing cognitive load and enhancing user satisfaction [51]. For patients, the platform offers a personalised health portal where they can view their medical history, prescriptions, and lab results in an organized, comprehensible format [52]. The design emphasizes minimalist aesthetics with consistent colour palettes, readable fonts, and iconography that promotes calmness and clarity-particularly important for individuals who may be anxious about their health [53]. For healthcare providers, the dashboard integrates clinical decision support tools, real-time notifications, and simplified data entry features, helping them manage consultations efficiently without the burden of complex software [54]. Accessibility remains a key principle of the design. The platform complies with Web Content Accessibility Guidelines (WCAG) 2.1, ensuring compatibility with screen readers, keyboard navigation, and voice commands for users with disabilities [55]. Multilingual support and adjustable text sizes further enhance usability, allowing patients from different regions and literacy levels to access healthcare services seamlessly [56]. The interface design is also responsive across devices-from smartphones to desktops-enabling both doctors and patients to access the system anytime, anywhere [57]. To ensure continuous improvement, user feedback loops are integrated into the system, allowing real-time suggestions and usability testing to shape future updates [58]. The feedback mechanism empowers users to share their experiences, which are then analysed through human-computer interaction (HCI) models to refine navigation and eliminate friction points [59]. Additionally, the platform undergoes regular usability audits using tools like SUS (System Usability Scale) and heuristic evaluations to maintain global usability standards [60]. Ultimately, the website’s design philosophy revolves around “designing for empathy”-understanding user needs, emotions, and challenges-to create a digital healthcare environment that feels safe, accessible, and empowering for everyone involved [49,60].

6. RISK ASSESSMENT & THREAT LANDSCAPE:

In digital healthcare systems, safeguarding patient data involves more than just encryption or secure servers-it requires an ongoing understanding of evolving cybersecurity threats and proactive risk management [62]. The website incorporates a comprehensive risk assessment framework to identify, evaluate and mitigate potential threats across technical, procedural, and human layers of operation [63]. Among the most common risks in healthcare data systems are insider misuse, network breaches, ransomware attacks, phishing attempts, device vulnerabilities, and outdated legacy systems [64]. Insider threats, whether intentional or accidental, pose a significant risk to data confidentiality and integrity. To counter these, the platform uses role-based access control (RBAC) and detailed activity logs that track every user action in real time, ensuring accountability [65]. Additionally, access permissions are regularly reviewed to prevent privilege escalation and unauthorized access to sensitive patient information [66]. Network breaches and ransomware attacks remain among the most destructive forms of cyber threats in healthcare [67]. To minimize such risks, the system integrates intrusion detection and prevention systems (IDPS) that continuously monitor incoming traffic for suspicious behavior [68]. Data backups are encrypted and stored in geographically redundant servers, ensuring that operations can recover swiftly even in the event of a breach [69]. Multi-layered firewall protection, regular security patching, and the use of secure socket layer (SSL) protocols safeguard communication channels from external intrusions [70]. Phishing and social engineering attacks are addressed through human-centric security training programs for healthcare professionals and administrative users, raising awareness about fraudulent emails, credential theft and deceptive links [71]. Endpoint protection is implemented to secure devices such as tablets and workstations used for patient data entry, ensuring that malware or unauthorized software cannot compromise system integrity [72]. The incident response mechanism of the website follows a structured approach: detection, containment, notification and recovery [73]. Once an anomaly is detected, the security operations module isolates affected segments to prevent lateral spread. Simultaneously, users and authorities are notified in compliance with privacy regulations such as HIPAA and GDPR [74]. Post-incident, forensic analysis helps identify vulnerabilities and update system policies to prevent recurrence. While security remains a top priority, it often involves trade-offs between protection and usability and between cost and practicality [75]. Excessive security layers can slow down performance or complicate user workflows, whereas minimal safeguards increase exposure to risk. The website balances these by adopting adaptive security models, which dynamically adjust protection levels based on risk context and user role, thus maintaining usability without compromising safety [76]. Overall, by merging robust cybersecurity practices with user-oriented design, the system achieves a balance between resilience, reliability, and practicality-qualities essential for sustaining trust in digital healthcare ecosystems [62,64,76].

7. EVALUATION METRICS & OUTCOMES:

To ensure that the website performs effectively as a secure and user-friendly digital healthcare platform, systematic evaluation metrics have been established to measure both technical performance and user satisfaction [77]. The success of the platform is gauged through measurable indicators such as the number of active users, uptime percentage, system response time, data retrieval speed, and user engagement rate [78]. These metrics help determine whether the system meets the operational expectations of healthcare providers and patients alike. From a security standpoint, one of the primary success indicators is the absence of data breaches or unauthorized access incidents, which reflects the strength of the implemented cybersecurity measures [79]. Regular monitoring of failed login attempts, intrusion detection system (IDS) alerts, and access anomalies provides continuous insights into the system's defensive posture [80]. In addition, audit log counts are analyzed periodically to verify the frequency and legitimacy of user interactions, helping identify irregular patterns that may indicate potential misuse [81]. User satisfaction is another core metric that defines the real-world effectiveness of the platform. Periodic surveys and feedback forms assess dimensions such as ease of navigation, system reliability, information accessibility, and visual appeal [82]. The results are quantified using standardized evaluation tools such as the System Usability Scale (SUS) and the Net Promoter Score (NPS) to track satisfaction trends over time [83]. From a data management perspective, data retrieval error rates and time to access patient records are closely monitored to ensure the efficiency of the backend architecture [84]. Faster access with minimal latency demonstrates optimized database indexing and caching strategies, while low retrieval error rates indicate the accuracy and integrity of stored information [85]. For security posture monitoring, the system maintains a live threat intelligence dashboard, displaying statistics such as the number of unauthorized access attempts blocked, vulnerabilities identified, and patches successfully deployed [86]. Continuous vulnerability assessments, penetration testing, and risk audits are performed quarterly to ensure adherence to the latest cybersecurity standards [87]. The philosophy of continuous improvement forms the backbone of the platform's long-term sustainability. Regular software updates, feature enhancements, and security patches are scheduled based on evolving cyber threats and user feedback [88]. A DevSecOps model is adopted, integrating security considerations directly into the development cycle to ensure that every system update maintains compliance, security, and efficiency [89]. Furthermore, user feedback is continuously collected and analyzed using data analytics models to refine usability, accessibility, and responsiveness [90]. Through these combined quantitative and qualitative evaluation metrics, the website not only demonstrates its reliability and resilience but also establishes a cycle of ongoing improvement, aligning technology performance with the ethical and operational demands of modern healthcare [77,88,90].

8. CHALLENGES, LIMITATIONS & FUTURE DIRECTIONS:

Despite its strengths in securing and managing patient data efficiently, the healthcare management website currently faces a few practical and structural challenges that influence its scalability and adoption [91]. One of the primary limitations lies in integration with legacy hospital information systems, which often rely on outdated or incompatible formats, making seamless data exchange difficult [92]. This interoperability gap can lead to data redundancy or errors when merging patient records across multiple institutions [93]. Another significant limitation is the cost associated with infrastructure maintenance and cybersecurity compliance. Implementing secure cloud servers, periodic penetration testing, and encryption protocols demand substantial financial and technical resources, which can be burdensome for small healthcare providers [94]. Additionally, user adoption among healthcare workers can be slow due to limited digital literacy, resistance to change, or fear of technological complexity [95]. This highlights the need for ongoing training and capacity-building programs to ensure that both patients and professionals can fully benefit from the system [96]. Connectivity issues in rural or low-resource areas also pose a barrier to consistent use, as real-time data synchronization and teleconsultation require stable internet access [97]. In regions with weak infrastructure, this may cause delays in updating medical records or accessing emergency information. Moreover, trust and privacy concerns remain critical—patients may hesitate to share sensitive data online due to the perceived risk of misuse or breaches, despite technical safeguards [98]. Building transparent data governance policies and clear consent mechanisms will therefore be essential to strengthening user confidence. Looking forward, several future enhancements are planned to overcome these barriers and advance the platform's intelligence and reliability. Integration of artificial intelligence (AI) for anomaly detection can enable early recognition of suspicious activities, system errors, or potential breaches before they escalate [99]. Similarly, blockchain technology could be implemented to ensure transparent, tamper-proof logging of transactions, enhancing trust and accountability in medical data handling [100]. Another promising direction is federated learning, where machine learning models are trained across multiple decentralized datasets without centralizing patient data, ensuring both privacy and analytical power [101]. The platform also envisions integration with IoT-enabled medical devices and wearable technologies to enable real-time health monitoring and personalized care [102]. Such connectivity would empower patients to track their vitals continuously while allowing healthcare professionals to make proactive interventions based on real-time analytics [103]. To ensure long-term sustainability, the website will adopt a structured framework for maintenance, governance, and financial viability. Routine updates and audits will be managed by a dedicated technical team, ensuring security compliance with evolving standards like HIPAA and GDPR [104]. Establishing a governance board composed of healthcare professionals, data scientists, and IT experts will maintain accountability and transparency in decision-making [105]. Additionally, partnerships with government health programs and academic institutions can support funding continuity, while periodic training sessions will keep end-users skilled and adaptive to upgrades [106]. Through continuous innovation, ethical oversight, and community collaboration, the system aims to evolve into a holistic, intelligent, and sustainable digital healthcare ecosystem that aligns with the global vision of secure and equitable health data management [91,105,106].

CONCLUSION

The development of PharmaHealthia represents a significant step toward achieving secure, efficient, and patient-centric healthcare digitalization [107]. The platform consolidates multiple healthcare processes-ranging from electronic medical record (EMR) management and pharmacy integration to data security and analytics-into a single, unified ecosystem [108]. By centralizing these functions, it enhances coordination among healthcare providers, reduces redundancies, and ensures that critical patient information is both accessible and protected [109]. At its core, PharmaHealthia embodies the principles of data privacy, transparency, and interoperability, which are increasingly recognized as the foundation of trustworthy digital health systems [110]. The use of robust encryption protocols, role-based access control, and continuous monitoring fosters a strong cybersecurity posture, addressing concerns of unauthorized access and data breaches that have long challenged healthcare organizations [111]. Moreover, the platform prioritizes user empowerment by offering patients control over their medical data while facilitating healthcare professionals with real-time insights for improved decision-making. This dual-benefit design supports the broader objective of patient-centered care, aligning with global health informatics trends that emphasize engagement, accessibility, and personalization. Despite these advancements, challenges such as integration with legacy systems, limited digital literacy among users, and infrastructural disparities in rural regions remain to be addressed. Future iterations of PharmaHealthia will integrate artificial intelligence (AI) for predictive analytics, blockchain for transparent data exchange, and federated learning to enhance privacy-preserving collaboration among healthcare networks. These features aim to further strengthen trust, scalability, and system intelligence while ensuring compliance with ethical and regulatory frameworks. Sustainability will depend on ongoing training programs, policy governance, and strategic funding collaborations to maintain operational excellence and ethical oversight. By continuously evolving with user feedback, technological innovation, and robust data governance, PharmaHealthia aspires to become a benchmark in secure digital healthcare ecosystems, promoting efficiency, accessibility, and patient trust on a global scale.

REFERENCES

1. Persson J, Rydenfält C. Why are digital health care systems still poorly designed, and why is health care practice not asking for more? Three paths toward a sustainable digital work environment. Journal of Medical Internet Research. 2021 Jun 22;23(6):e26694.
2. Cripps M, Scarbrough H. Making digital health “solutions” sustainable in healthcare systems: a practitioner perspective. Frontiers in digital health. 2022 Mar 31;4:727421.
3. Naik N, Hameed BZ, Sooriyaperakasam N, Vinayahalingam S, Patil V, Smriti K, Saxena J, Shah M, Ibrahim S, Singh A, Karimi H. Transforming healthcare through a digital revolution: a review of digital healthcare technologies and solutions. Frontiers in digital health. 2022 Aug 4;4:919985.
4. Clausen A, Christensen ER, Jakobsen PR, Søndergaard J, Abrahamsen B, Rubin KH. Digital solutions for decision support in general practice–a rapid review focused on systems developed for the universal healthcare setting in Denmark. BMC Primary Care. 2023 Dec 14;24(1):276.
5. Akinola S, Telukdarie A. Sustainable digital transformation in healthcare: Advancing a digital vascular health innovation solution. Sustainability. 2023 Jul 1;15(13):10417.
6. Singh S, Sharma P. Challenges and Opportunities of Digital Public Health. Indian Journal of Health Sciences and Care. 2024 May 1;11(2):51-6.
7. Chen AM. Crossing the digital chasm: a narrative review on how technology can improve healthcare access. Journal of Hospital Management and Health Policy. 2024 Dec 30;8.
8. Naik N, Hameed BZ, Sooriyaperakasam N, Vinayahalingam S, Patil V, Smriti K, Saxena J, Shah M, Ibrahim S, Singh A, Karimi H. Transforming healthcare through a digital revolution: a review of digital healthcare technologies and solutions. Frontiers in digital health. 2022 Aug 4;4:919985.
9. Madanian S, Nakarada-Kordic I, Reay S, Chetty TH. Patients' perspectives on digital health tools. PEC innovation. 2023 Dec 1;2:100171.
10. Maita KC, Maniaci MJ, Haider CR, Avila FR, Torres-Guzman RA, Borna S, Lunde JJ, Coffey JD, Demaerschalk BM, Forte AJ. The impact of digital health solutions on bridging the health care gap in rural areas: a scoping review. The Permanente Journal. 2024 Aug 13;28(3):130.
11. Santonen T, Petsani D, Julin M, Garschall M, Kropf J, Van der Auwera V, Bernaerts S,

Losada R, Almeida R, Garatea J, Muñoz I. Cocreating a Harmonized Living Lab for Big Data–Driven Hybrid Persona Development: Protocol for Cocreating, Testing, and Seeking Consensus. JMIR Research Protocols. 2022 Jan 6;11(1):e34567.

12. Naik N, Hameed BZ, Sooriyaperakasam N, Vinayahalingam S, Patil V, Smriti K, Saxena J, Shah M, Ibrahim S, Singh A, Karimi H. Transforming healthcare through a digital revolution: a review of digital healthcare technologies and solutions. Frontiers in digital health. 2022 Aug 4;4:919985.
13. Catapan SC, et al. Trust, Privacy, and Ethical Considerations in Digital Health Systems. NPJ Digital Medicine. 2025;8:45. doi:10.1038/s41746-025-0045-3.
14. Naik N, Hameed BZ, Sooriyaperakasam N, Vinayahalingam S, Patil V, Smriti K, Saxena J, Shah M, Ibrahim S, Singh A, Karimi H. Transforming healthcare through a digital revolution: a review of digital healthcare technologies and solutions. Frontiers in digital health. 2022 Aug 4;4:919985.
15. AlRyalat S, Al-Sheikh O, Al-Yousef A. Secure data management in digital healthcare: Trends and frameworks. JMIR Med Inform. 2023;11:e47561. doi:10.2196/47561.
16. Asha K, Kumar P, Bansal M. Role-based access control in health information systems: A systematic review. Health Inf Sci Syst. 2024;12:45. doi:10.1007/s13755-024-00345-y.
17. Santonen T, Petsani D, Julin M, Garschall M, Kropf J, Van der Auwera V, Bernaerts S, Losada R, Almeida R, Garatea J, Muñoz I. Cocreating a Harmonized Living Lab for Big Data–Driven Hybrid Persona Development: Protocol for Cocreating, Testing, and Seeking Consensus. JMIR Research Protocols. 2022 Jan 6;11(1):e34567.
18. Natsiavas P, et al. Interoperability and modularity in healthcare IT systems: A European perspective. BMC Med Inform Decis Mak. 2022;22:311. doi:10.1186/s12911-022-01935-2.
19. Manogaran G, et al. Blockchain-based audit trails for secure health data management. Comput Electr Eng. 2023;110:108789. doi:10.1016/j.compeleceng.2023.108789.
20. Mateus Ferreira AM, Alho I, Neves AL, Lopes H, Correia M. “First, Do No Harm” in the Digital Era: Examining the Practicality of the European Health Data Space Proposal and Ethical Implications of Artificial Intelligence. A Systematic Literature Review. the Digital Era: Examining the Practicality of the European Health Data Space Proposal and Ethical Implications of Artificial Intelligence. A Systematic Literature Review.
21. Shakor MY, Khaleel MI. Recent advances in big medical image data analysis through deep learning and cloud computing. Electronics. 2024 Dec 10;13(24):4860.
22. Gider J, Renneboog L, Strauss T. The Regulation of Data Privacy and Cybersecurity. European Corporate Governance Institute-Law Working Paper. 2025 Jul 1(853).
23. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: A comprehensive review and directions for future research. IEEE Access. 2022;10:98830–98855.
24. Patel V, et al. Secure cloud-based healthcare storage systems: A systematic review. IEEE Access. 2023;11:103213-103229.
25. Cavoukian A. Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario; 2021.

26. Naik N, Hameed BMZ, Sooriyaperakasam N, et al. Transforming healthcare through digital platforms. Front Digit Health. 2022;4:919985.
27. Zubaydi H, Alenezi M, Ameen N. Cybersecurity awareness among healthcare professionals: A narrative review. Health Informatics J. 2023;29(4):14604582231222311.
28. Ramesh R, Ganesan M, Gupta S. Ethical dimensions of healthcare data privacy in the digital age. BMC Med Ethics. 2023;24(1):115.
29. Mehta V, Sharma R, Agarwal A. Legal landscape of digital health data in India: Compliance with DPDP Act 2023. Indian J Med Ethics. 2024;9(2):45–51.
30. Ministry of Electronics and Information Technology, Government of India. Digital Personal Data Protection Act, 2023 and IT Rules, 2011.
31. Martínez-Pérez B, De la Torre-Díez I, López-Coronado M. Privacy and security in healthcare apps under HIPAA and GDPR. Int J Environ Res Public Health. 2022;19(12):7248.
32. Catapan SC, et al. Trust, privacy, and ethical considerations in digital health systems. NPJ Digit Med. 2025;8:45.
33. Alshahrani A, et al. Continuous compliance monitoring in digital health systems. Front Digit Health. 2022;4:921045.
34. Beauchamp TL, Childress JF. Principles of Biomedical Ethics. 8th ed. Oxford University Press; 2021.
35. European Data Protection Board. Guidelines on the Right to Data Portability under GDPR. 2022.
36. Alotaibi Y, Almalki H, Basamh S. End-to-end encryption for patient data protection: Current challenges and future perspectives. Health Technol (Berl). 2023;13(2):217–227.
37. Rashid H, et al. Equity and inclusion in digital health: Addressing barriers to access. BMJ Glob Health. 2024;9(3):e013229.
38. Mirkovic J, et al. Responsive design and mobile health: Trends in patient engagement. JMIR Form Res. 2023;7:e45789.
39. Kruse CS, Stein A, Thomas H. The digital divide in healthcare: Implications for access and quality. J Telemed Telecare. 2023;29(7):422–431.
40. Mittelstadt BD. Principles of algorithmic fairness in healthcare AI. Ethics Inf Technol. 2022;24:58–70.
41. Naik N, Hameed BMZ, Sooriyaperakasam N, et al. Transforming healthcare through digital platforms: Opportunities and challenges. Front Digit Health. 2022;4:919985.
42. Wilson P, Greenhalgh T, Shaw S. The importance of user experience in digital healthcare adoption. JMIR Hum Factors. 2023;10(2):e45321.
43. Zhang X, Yang Y, Li L. Human-centred design for digital health interventions: A systematic review. Int J Med Inform. 2024;180:105224.
44. Lee J, Park H, Kim J. User interface design patterns for electronic health records: A review. BMC Med Inform Decis Mak. 2023;23:118.
45. Boudreaux ED, Cohn A, Gardiner P. Patient portals and engagement: Current perspectives. Patient Exp J. 2022;9(3):27-36.
46. Duarte A, Oliveira R, Pereira J. Design aesthetics in healthcare user interfaces: Emotional and cognitive impacts. Health Technol (Berl). 2023;13:333–345.
47. Li J, Ray P, Choi J. Clinical decision support interfaces for physicians: A usability

perspective. J Biomed Inform. 2023;144:104421.
48. World Wide Web Consortium (W3C). Web Content Accessibility Guidelines (WCAG) 2.1. 2021.
49. Martínez-Millana A, et al. Enhancing multilingual usability in health portals: A cross-cultural study. Int J Environ Res Public Health. 2023;20(8):5221.
50. Mirkovic J, et al. Responsive design and mobile health: Trends in patient engagement. JMIR Form Res. 2023;7:e45789.
51. Alshahrani A, et al. Continuous feedback mechanisms in digital healthcare systems. Front Digit Health. 2022;4:921045.
52. Kim H, et al. Human–computer interaction in eHealth systems: Design implications. Interact J Med Res. 2023;12:e44211.
53. Nielsen J. Usability Engineering. Academic Press; 2022.
54. Norman DA. The Design of Everyday Things. MIT Press; 2021.
55. Momen N, Alqahtani M, Abbas R. Digital resilience in healthcare: Security, privacy, and ethics. Front Digit Health. 2023;5:102214.
56. Vora J, Shah M, Parikh S. Framework for healthcare cyber risk assessment and management. Health Informatics J. 2023;29(2):14604582231115622.
57. Kruse CS, Frederick B, Jacobson T. Cybersecurity in healthcare: A systematic review of modern threats and preventive strategies. JMIR Med Inform. 2022;10(3):e34352.
58. Asha K, Kumar P, Bansal M. Role-based access control in health information systems: A systematic review. Health Inf Sci Syst. 2024;12:45.
59. Patel V, et al. Secure cloud-based healthcare storage systems: A systematic review. IEEE Access. 2023;11:103213–103229.
60. Anwar S, Rahman M, Cho G. Ransomware in healthcare: Threats and countermeasures. J Cybersecur Priv. 2023;3(1):55–73.
61. Kim J, Lee H, Park Y. Intrusion detection systems for e-health networks: Trends and challenges. Comput Secur. 2024;139:103675.
62. Manogaran G, Thota C, Lopez D. Blockchain-based audit trails for secure health data management. Comput Electr Eng. 2023;110:108789.
63. Li M, Chen X, Liu Q. Multi-layered cybersecurity architecture for health information systems. Comput Methods Programs Biomed. 2024;251:108923.
64. Zubaydi H, Alenezi M, Ameen N. Cybersecurity awareness among healthcare professionals: A narrative review. Health Informatics J. 2023;29(4):14604582231222311.
65. Wang X, et al. Device security and endpoint protection in telemedicine environments. IEEE Access. 2022;10:97432–97445.
66. Naik N, Hameed BMZ, Sooriyaperakasam N, et al. Transforming healthcare through digital platforms: Opportunities and challenges. Front Digit Health. 2022;4:919985.
67. Martínez-Pérez B, De la Torre-Díez I, López-Coronado M. Privacy and security in healthcare apps under HIPAA and GDPR. Int J Environ Res Public Health. 2022;19(12):7248.
68. Norman DA. The Design of Everyday Things. MIT Press; 2021.
69. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: A comprehensive review and directions for

future research. IEEE Access. 2022;10:98830–98855.

70. Davis FD, Taylor S, Damschroder LJ. Evaluation frameworks for digital health implementation success. JMIR Med Inform. 2023;11:e45562.
71. Lee J, Park H, Kim J. User interface performance metrics in digital health platforms. BMC Med Inform Decis Mak. 2023;23:118.
72. Kruse CS, Frederick B, Jacobson T. Cybersecurity in healthcare: A systematic review of modern threats and preventive strategies. JMIR Med Inform. 2022;10(3):e34352.
73. Kim J, Lee H, Park Y. Intrusion detection systems for e-health networks: Trends and challenges. Comput Secur. 2024;139:103675.
74. Manogaran G, Thota C, Lopez D. Blockchain-based audit trails for secure health data management. Comput Electr Eng. 2023;110:108789.
75. Boudreaux ED, Cohn A, Gardiner P. Patient portals and engagement: Current perspectives. Patient Exp J. 2022;9(3):27–36.
76. Nielsen J. Usability Engineering. Academic Press; 2022.
77. Patel V, et al. Secure cloud-based healthcare storage systems: A systematic review. IEEE Access. 2023;11:103213–103229.
78. Li M, Chen X, Liu Q. Multi-layered cybersecurity architecture for health information systems. Comput Methods Programs Biomed. 2024;251:108923.
79. Naik N, Hameed BMZ, Sooriyaperakasam N, et al. Transforming healthcare through digital platforms: Opportunities and challenges. Front Digit Health. 2022;4:919985.
80. Zubaydi H, Alenezi M, Ameen N. Cybersecurity awareness among healthcare professionals: A narrative review. Health Informatics J. 2023;29(4):14604582231222311.
81. Vora J, Shah M, Parikh S. Framework for healthcare cyber risk assessment and management. Health Informatics J. 2023;29(2):14604582231115622.
82. Kumar R, Gupta N, Singh M. DevSecOps in digital health infrastructure: Bridging security and agility. IEEE Access. 2024;12:21794–21810.
83. Alshahrani A, et al. Continuous feedback mechanisms in digital healthcare systems. Front Digit Health. 2022;4:921045.
84. Kruse CS, Frederick B, Jacobson T. Cybersecurity in healthcare: A systematic review of modern threats and preventive strategies. JMIR Med Inform. 2022;10(3):e34352.
85. Bouri N, Sheikh A, Anderson M. Overcoming legacy barriers in digital health integration. BMC Health Serv Res. 2023;23:248.
86. Alamo T, Reina DG, Mammarella M. Interoperability and data exchange challenges in healthcare systems. Health Informatics J. 2022;28(4):14604582221092711.
87. Li M, Chen X, Liu Q. Multi-layered cybersecurity architecture for health information systems. Comput Methods Programs Biomed. 2024;251:108923.
88. Cresswell KM, Williams R, Sheikh A. Adopting electronic health records: Lessons from sociotechnical perspectives. J Am Med Inform Assoc. 2023;30(1):120–128.
89. Vora J, Shah M, Parikh S. Framework for healthcare cyber risk assessment and management. Health Informatics J. 2023;29(2):14604582231115622.

90. Naik N, Hameed BMZ, Sooriyaperakasam N, et al. Transforming healthcare through digital platforms: Opportunities and challenges. Front Digit Health. 2022;4:919985.
91. Menachemi N, Rahurkar S, Harle CA. Privacy and trust in digital health data ecosystems. Health Aff (Millwood). 2022;41(6):892–901.
92. Kumar R, Gupta N, Singh M. DevSecOps and AI in digital health infrastructure: Bridging security and agility. IEEE Access. 2024;12:21794–21810.
93. Manogaran G, Thota C, Lopez D. Blockchain-based audit trails for secure health data management. Comput Electr Eng. 2023;110:108789.
94. Yang Q, Liu Y, Chen T. Federated learning for healthcare data privacy. Nat Mach Intell. 2023;5(1):5–12.
95. Hossain MS, Muhammad G, Rahman M. IoT-enabled smart healthcare: A comprehensive review. IEEE Internet Things J. 2023;10(4):3542–3556.
96. Lee J, Park H, Kim J. User interface performance metrics in digital health platforms. BMC Med Inform Decis Mak. 2023;23:118.
97. Zubaydi H, Alenezi M, Ameen N. Cybersecurity awareness among healthcare professionals: A narrative review. Health Informatics J. 2023;29(4):14604582231222311.
98. Davis FD, Taylor S, Damschroder LJ. Evaluation frameworks for digital health implementation success. JMIR Med Inform. 2023;11:e45562.
99. Alshahrani A, et al. Continuous feedback mechanisms in digital healthcare systems. Front Digit Health. 2022;4:921045.
100. Naik N, Hameed BMZ, Sooriyaperakasam N, et al. Transforming healthcare through digital platforms: Opportunities and challenges. Front Digit Health. 2022;4:919985.
101. Bouri N, Sheikh A, Anderson M. Overcoming legacy barriers in digital health integration. BMC Health Serv Res. 2023;23:248.
102. Kruse CS, Frederick B, Jacobson T. Cybersecurity in healthcare: A systematic review of modern threats and preventive strategies. JMIR Med Inform. 2022;10(3):e34352.
103. Alamo T, Reina DG, Mammarella M. Interoperability and data exchange challenges in healthcare systems. Health Informatics J. 2022;28(4):14604582221092711.
104. Li M, Chen X, Liu Q. Multi-layered cybersecurity architecture for health information systems. Comput Methods Programs Biomed. 2024;251:108923.
105. Boudreaux ED, Cohn A, Gardiner P. Patient portals and engagement: Current perspectives. Patient Exp J. 2022;9(3):27–36.
106. Davis FD, Taylor S, Damschroder LJ. Evaluation frameworks for digital health implementation success. JMIR Med Inform. 2023;11:e45562.
107. Cresswell KM, Williams R, Sheikh A. Adopting electronic health records: Lessons from sociotechnical perspectives. J Am Med Inform Assoc. 2023;30(1):120–128.
108. Kumar R, Gupta N, Singh M. DevSecOps and AI in digital health infrastructure: Bridging security and agility. IEEE Access. 2024;12:21794–21810.
109. Manogaran G, Thota C, Lopez D. Blockchain-based audit trails for secure health data management. Comput Electr Eng. 2023;110:108789.

110. Alshahrani A, et al. Continuous feedback mechanisms in digital healthcare systems. Front Digit Health. 2022;4:921045.

111. Vora J, Shah M, Parikh S. Framework for healthcare cyber risk assessment and management. Health Informatics J. 2023;29(2):14604582231115622.

HOW TO CITE: Rohan Kaswa, Sakshi Kashid, Suyog Kamble, Aboli Kasar, Rutuja Kadam, Manisha Khaire, PharmaHealthia: One Stop Digital Solution for Patient and Healthcare, Int. J. of Pharm. Sci., 2026, Vol 4, Issue 2, 1567-1581. https://doi.org/10.5281/zenodo.18596929