Keywords
Information literacy; rural health; health decision-making; mobile health (mHealth); digital health literacy; patient trust; data privacy; privacy governance; health informatics; digital divide; health behavior; technology adoption; structural equation modeling.

Authors
"Maksudov Dilshod Davronovich.[1]
[1*]PhD. Assistent of Samarkand state medical university. dr.maqsudovdilshod@gmail.com. https://orcid.org/0009-0005-3464-4765"

"Azimova Shakhnoza Shukhratovna[2]
[2]PhD, Associate Professor. BUKHARA STATE MEDICAL INSTITUTE NAMED AFTER ABU ALI IBN SINO. e-mail: azimova.shaxnoza@bsmi.uz ORCID:0009-0009-9961-4398"

Omonova Guzal Zarifovna. [3]
[3]Assistant of the department of 1-Pediatrics and Neonatology Samarkand State Medical University. ORCID:0009000739544848 e-mail: omonovaguzal96@gmail.com

Yarmuxamedova Makhbuba Kudratovna[4]
[4]PhD in medical sciences, Associate Professor, Samarkand State Medical University, mahbubayarmuhamedova1955@gmail.com https://orcid.org/0009-0004-2038-5726

[5]Nosirova Lobar Rozikovna[5]
Teacher of the Departament Methodology of Teaching Foreign Languages at Bukhara State Pedagogical Institute
https://orcid.org/0009-0009-7068-7817
lobarnosir87@gmail.com

Rustamov Uktam Mardonkulovich[6]
[6]MD, Master of science, Department of Public Health and Healthcare Management of the Samarkand State Medical University Uktam.rustamov@gmail.com ORCID iD: 0009-0003-9218-4379

Received-17-05-2026
Revised-20-06-2026
Accepted-25-06-2026
Doi:10.1922/ejprd.v34i4s.1439

Information Literacy, Digital Trust, and Health Decision-Making in Rural Populations: Evaluating Privacy-Aware Engagement with Mobile Health Applications

Abstract
Background: Rural populations increasingly rely on mobile health (mHealth) applications to access healthcare information, monitor chronic conditions, and support self-care in settings where medical infrastructure is often limited. However, this growing dependence occurs alongside persistent deficits in information literacy and limited capacity to critically evaluate digital health content. As a result, individuals in rural contexts are particularly vulnerable to misinformation, suboptimal health decisions, and insufficient awareness of data privacy risks embedded in digital health ecosystems.
Objective: This study examines the interrelationship between information literacy, health decision-making, and perceived effectiveness of data privacy protections in mHealth applications. It seeks to understand how rural users interpret, trust, and act upon digital health information while engaging with platforms that collect and process sensitive personal data.
Methods:A mixed-methods research design was employed, integrating a structured survey of rural mHealth users, systematic privacy audits of widely used health applications, and behavioral modeling techniques. The survey assessed information literacy levels, trust in digital health systems, and health-related decision-making behaviors. App audits evaluated privacy practices including permission structures, encryption protocols, and third-party data sharing. Quantitative data were analyzed using regression and structural equation modeling to identify relationships between literacy, privacy perception, and adoption behavior.
Results: Findings indicate that higher information literacy is positively associated with improved health decision-making and greater critical awareness of privacy risks. However, trust in mHealth applications often mediates this relationship, with users demonstrating continued reliance on apps despite recognizing potential privacy vulnerabilities. Significant discrepancies were also observed between perceived and actual privacy protections across applications, particularly in wellness-oriented platforms.
Conclusion: The study highlights a complex interplay between information literacy, digital trust, and privacy governance in shaping rural health behaviors. Strengthening digital health literacy and improving transparency in mHealth privacy practices are essential for supporting equitable health decision-making and reducing vulnerability in underserved populations.

2. Introduction

Digital health has moved from being a supplementary component of healthcare delivery to a central infrastructure through which people access information, monitor symptoms, communicate with providers, and make everyday health decisions. The World Health Organization's *Global Strategy on Digital Health 2020–2025* frames digital technologies as essential to strengthening health systems, improving equity, and expanding access, particularly where conventional services remain geographically or

economically constrained (World Health Organization [WHO], 2021). This policy direction is especially relevant for rural populations, where shortages of healthcare professionals, long travel distances, fragmented referral pathways, and delayed access to specialist
care continue to shape health outcomes. In such settings, mobile health applications are increasingly presented as practical tools for self-care, medication adherence, symptom tracking, chronic disease management, preventive education, and remote engagement with health systems.

Yet the expansion of mobile health is not automatically synonymous with equitable healthcare transformation. Rural adoption of mHealth often occurs under conditions of uneven connectivity, limited digital infrastructure, lower health service density, and variable levels of digital and information literacy. Recent studies on rural digital health show that digital technologies may improve access and continuity of care, but their effectiveness depends heavily on users' ability to interpret health information, evaluate app credibility, and translate digital feedback into meaningful action (Lestari et al., 2024; Monteiro et al., 2025). In rural contexts, where face-to-face clinical guidance may be intermittent, health information obtained through mobile apps can carry disproportionate influence. A blood glucose notification, medication reminder, symptom-checker result, or lifestyle recommendation may become part of a patient's decision-making process long before a professional consultation is available.

This makes information literacy a foundational, but often underestimated, dimension of rural health decision-making. Information literacy in health contexts involves more than the ability to read medical content. It includes locating relevant information, judging its reliability, recognizing commercial or algorithmic bias, understanding uncertainty, and applying information appropriately within one's personal and social circumstances. Rural residents with limited access to trusted clinical intermediaries may rely on mobile apps, online forums, family networks, pharmacists, or community health workers to interpret health information. This layered information environment can support autonomy, but it can also generate confusion when app-based advice conflicts with local beliefs, provider instructions, or lived experience. As Coughlin et al. (2020) argue, health literacy is closely tied to social determinants of health; therefore, digital information literacy cannot be treated as an individual skill alone, but must be understood in relation to education, income, access, language, trust, and institutional support.

The issue becomes more complex when mHealth applications are used for chronic disease management. Rural populations often experience higher burdens of conditions such as diabetes, hypertension, cardiovascular disease, and respiratory illness, while also facing barriers to continuous care. Mobile apps can help users record symptoms, track medications, monitor physical activity, and receive reminders. However, the usefulness of these tools depends not only on technical availability but also on whether users can understand app-generated information and assess its relevance. A patient may receive a warning about blood pressure trends but lack the confidence to interpret the severity of the alert. Another may follow lifestyle guidance generated by a commercial app without knowing whether it is clinically validated.
In this sense, mHealth does not merely transmit health information; it reshapes the relationship between knowledge, trust, and decision-making.

At the same time, mHealth ecosystems introduce significant privacy and data governance risks. Health apps routinely collect sensitive personal data, including symptoms, medication use, reproductive information, location patterns, biometric indicators, behavioral data, and sometimes inferences about mental health or disease risk. Evidence from app privacy studies suggests that data sharing with third parties remains common and often poorly disclosed. Grundy et al. (2019) found that medicines-related apps frequently shared user data with external entities, while Tangari et al. (2021) reported widespread privacy concerns across thousands of health-related Android apps, including inconsistent privacy practices and extensive data collection. These findings are particularly troubling in rural contexts because privacy harms may have heightened social consequences. In smaller communities, disclosure or misuse of health information may affect not only individual autonomy but also social reputation, employment, insurance access, family relationships, and willingness to seek care.

Existing regulatory frameworks provide important but incomplete protection. The General Data Protection Regulation (GDPR) establishes strong principles around consent, data minimization, transparency, and individual rights in the European context. HIPAA protects health information handled by covered entities and their business associates in the United States. However, both frameworks encounter limitations when applied to consumer-facing mHealth environments. HIPAA does not generally protect information voluntarily entered into mobile apps that are not offered by or on behalf of regulated healthcare entities, even when the information is health-related (U.S. Department of Health and Human Services, 2024). In response to this regulatory gap, the U.S. Federal Trade Commission updated its Health Breach Notification Rule in 2024 to clarify its application to health apps and similar technologies not covered by HIPAA (Federal Trade Commission, 2024). These developments show that privacy governance is evolving, but they also reveal a persistent mismatch between legal categories and everyday digital health practices.

For rural users, the consequences of this mismatch are not merely legal or technical. Privacy policies are often

long, abstract, and difficult to interpret, even for digitally confident users. For individuals with limited information literacy, meaningful consent may be reduced to clicking "agree" without understanding what data are collected, how they are shared, or what risks may follow. Privacy vulnerability therefore intersects with the digital divide. The rural digital divide is not only a matter of internet access or device ownership; it also includes uneven capacity to evaluate digital tools, negotiate privacy choices, and challenge opaque data practices. A rural patient may adopt an app because it is affordable and accessible, yet remain unaware that the same app may monetize behavioral or health-related data. This creates an asymmetry in which the populations most likely to benefit from accessible digital health tools may also be among the least equipped to assess their risks.

This study is positioned at the intersection of information literacy, rural health decision-making, and mHealth data privacy governance. Existing research has examined digital health adoption, health literacy, and app privacy as partly separate fields. However, fewer studies have theorized how these dimensions interact in rural populations, where health decisions are shaped by constrained access, trust in digital tools, and limited visibility into data practices. The theoretical contribution of this study lies in reframing privacy-aware mHealth engagement as a form of situated information literacy.

From this perspective, the capacity to use mobile health apps responsibly is not limited to technical skill or health knowledge; it also includes the ability to interpret data practices, assess institutional trustworthiness, and make health decisions under conditions of informational and regulatory uncertainty.

Accordingly, this manuscript addresses the following research questions: **(1)** How does information literacy influence rural users' engagement with mobile health applications for self-care and chronic disease decision-making? **(2)** How do rural users perceive and negotiate privacy risks in mHealth ecosystems? **(3)** In what ways do current privacy governance frameworks support or fail to support privacy-aware mHealth engagement in rural contexts? The objectives are to develop an interdisciplinary account of rural mHealth use, identify the literacy and governance conditions that shape digital trust, and generate policy-relevant insights for designing privacy-aware, equitable, and context-sensitive digital health interventions.

3. Literature Review

The rapid integration of digital technologies into healthcare systems has generated a substantial body of research examining health literacy, digital engagement, data governance, and technology-mediated decision-making. However, much of this scholarship remains fragmented across disciplinary boundaries. Studies in health communication often emphasize literacy and patient empowerment, while information systems research prioritizes adoption behavior and usability. Privacy scholarship, meanwhile, tends to focus on legal compliance or technical protection mechanisms rather than the lived realities of vulnerable populations. Rural digital health research occupies an especially underdeveloped intersection within these domains. Although mobile health technologies are frequently promoted as tools for overcoming healthcare inequities, the relationship between information literacy, digital trust, and privacy-aware decision-making in rural contexts remains insufficiently theorized and empirically integrated.

Information Literacy and Health Literacy in Rural Contexts

Health literacy has evolved from a narrow understanding of reading and comprehension toward a multidimensional construct encompassing cognitive, social, and digital capacities. Sørensen et al. (2021) argue that contemporary health literacy includes the ability to access, interpret, evaluate, and apply health information within increasingly digitized environments. In parallel, information literacy research emphasizes evaluative judgment, critical interpretation, and contextual reasoning rather than simple information retrieval. These perspectives converge in digital health settings where patients must assess the credibility of mobile applications, understand algorithmically generated recommendations, and navigate privacy disclosures.

In rural populations, however, literacy-related challenges are shaped by structural inequalities rather than merely individual skill deficits. Research published in *JMIR mHealth and uHealth* and *BMC Digital Health* consistently demonstrates that rural residents often experience lower levels of digital health literacy due to educational disparities, limited broadband access, aging demographics, and reduced exposure to digital services (Levy et al., 2023; Neter & Brainin, 2022). Yet empirical evidence also complicates simplistic assumptions that rural populations are technologically resistant. Several studies show relatively high willingness to use mHealth tools when they are perceived as accessible, affordable, and clinically useful (Kim et al., 2022). This contradiction reveals an important distinction between adoption and meaningful engagement. A patient may download a health application without possessing the interpretive capacity necessary to evaluate medical accuracy, data collection practices, or algorithmic limitations. Consequently, digital participation does not necessarily translate into informed decision-making. Research in *The Lancet Digital Health* has increasingly emphasized this gap between technological availability and effective health agency, particularly among marginalized populations (Kickbusch et al., 2021).

Another recurring issue concerns the assumption that digital literacy naturally improves through repeated technological exposure. While prolonged use may increase familiarity with interfaces, it does not automatically strengthen critical understanding of data governance or information quality. This is especially significant in mHealth ecosystems where interfaces are intentionally simplified to maximize engagement.

Users may therefore become operationally competent while remaining informationally vulnerable. Such findings challenge technologically deterministic narratives suggesting that access alone can resolve rural health disparities.

Digital Health Adoption Models: TAM, UTAUT, and Privacy Calculus

Theoretical models explaining digital technology adoption have heavily influenced health informatics research.

The Technology Acceptance Model (TAM), originally proposed by Davis (1989), remains widely used in mHealth studies. TAM suggests that perceived usefulness and perceived ease of use determine user acceptance of technology. In rural healthcare contexts, studies applying TAM frequently identify convenience, reduced travel costs, and faster access to information as major drivers of mHealth adoption (Hoque & Sorwar, 2019).

However, critics argue that TAM inadequately captures sociocultural and ethical dimensions relevant to vulnerable populations. The model assumes relatively rational and individualized decision-making processes while underestimating structural inequalities, institutional trust, and informational asymmetry. For rural users, decisions regarding digital health technologies are often embedded within collective experiences, community norms, and constrained healthcare infrastructures. A patient may adopt a mobile app not because it is trusted, but because alternatives are inaccessible.

The Unified Theory of Acceptance and Use of Technology (UTAUT) expanded earlier models by incorporating social influence, facilitating conditions, and behavioral intention (Venkatesh et al., 2003). Recent health informatics studies have adapted UTAUT to explain telemedicine and mHealth adoption during and after the COVID-19 pandemic. Findings from *NPJ Digital Medicine* suggest that social endorsement by healthcare professionals significantly affects adoption among older and rural populations (Aji et al., 2023). This indicates that institutional trust remains central even within highly individualized digital environments.

Nevertheless, adoption frameworks continue to face limitations when addressing privacy-related behavior. Privacy calculus theory attempts to explain how individuals weigh perceived benefits against privacy risks when deciding whether to disclose personal information. In mHealth settings, users may tolerate extensive data collection if they believe the technology improves convenience or health outcomes. Yet empirical evidence repeatedly demonstrates a "privacy paradox," wherein individuals express concern about privacy while continuing to use data-intensive applications (Kokolakis, 2017).

Within rural populations, this paradox may be intensified by healthcare scarcity. When healthcare access is limited, users may perceive privacy compromise as unavoidable rather than acceptable. This distinction is theoretically important. Existing models often interpret continued usage as evidence of trust or satisfaction, whereas rural users may instead engage in forms of constrained acceptance driven by necessity. Such dynamics remain insufficiently addressed in mainstream digital health adoption literature.

Health Privacy Risks and Governance Frameworks

Privacy concerns have become one of the most debated dimensions of digital health governance. Mobile health applications routinely collect sensitive information including geolocation data, reproductive histories, behavioral metrics, mental health indicators, and biometric records. Multiple studies published in *BMJ*, *JMIR*, and *NPJ Digital Medicine* demonstrate that many health applications share user data with advertisers, analytics companies, or third-party intermediaries without transparent disclosure (Grundy et al., 2019; Tangari et al., 2021).

Importantly, privacy risks extend beyond data breaches. Scholars increasingly emphasize inferential privacy harms, where seemingly non-sensitive data can be combined to generate predictive profiles regarding illness, pregnancy, psychological vulnerability, or socioeconomic status. In rural communities, such risks may carry amplified consequences due to social visibility and reduced anonymity. Disclosure of stigmatized conditions within tightly interconnected social environments can affect employment, insurance access, or community relationships.

Governance frameworks such as GDPR and HIPAA attempt to establish legal protections for personal health information.

GDPR emphasizes informed consent, transparency, data minimization, and the right to data portability or erasure. HIPAA regulates protected health information handled by covered healthcare entities. Despite their significance, scholars have repeatedly identified limitations in both systems when applied to commercial mHealth ecosystems.

First, many consumer health applications fall outside HIPAA coverage because they are not formally connected to healthcare providers or insurers (Cohen & Mello, 2020). Second, GDPR's consent-centered model assumes that users can meaningfully understand privacy disclosures. Yet empirical studies show that privacy policies remain inaccessible for many users due to technical language, excessive length, and legal abstraction (Obar & Oeldorf-Hirsch, 2020). These challenges are likely intensified in rural populations with limited digital literacy.

Recent governance scholarship has therefore shifted toward broader concepts such as data justice, participatory governance, and ethical digital infrastructure. Rather than framing privacy as an individual responsibility, these approaches examine power asymmetries between users, platforms, healthcare systems, and data economies. In *The Lancet Digital Health*, researchers increasingly argue that digital health ethics must move beyond procedural

consent toward structural accountability and equitable governance (Morley et al., 2020).

Rural–Urban Disparities in Digital Health Access and Trust

The digital divide has traditionally been conceptualized as unequal access to internet infrastructure and digital devices. Contemporary scholarship, however, increasingly recognizes second-level and third-level divides involving differences in digital skills, usage quality, and outcomes. Rural populations may possess smartphones and internet connectivity while still lacking the institutional support necessary for informed and confident digital engagement.

Empirical studies across *JMIR*, *Frontiers in Digital Health*, and *NPJ Digital Medicine* demonstrate persistent rural–urban disparities in telemedicine use, app engagement, and trust in digital healthcare systems (Campos-Castillo & Anthony, 2021). Rural users often report lower confidence in app accuracy, reduced understanding of data practices, and concerns about surveillance or misuse. At the same time, they may rely more heavily on mHealth due to provider shortages and transportation barriers.

Trust therefore emerges as both enabling and problematic. Some studies indicate that institutional affiliation with hospitals or government health agencies improves user confidence in digital tools. Others show that familiarity with local healthcare providers remains more influential than platform design itself. Rural trust in digital health is often relational rather than technological; users may trust an application because it was recommended by a known clinician, pharmacist, or community worker.

However, trust does not necessarily correlate with actual privacy protection. Numerous widely trusted health apps have been found to engage in opaque data-sharing practices. This creates a critical contradiction within the literature: users often interpret usability, familiarity, or institutional branding as indicators of privacy safety despite lacking evidence regarding actual data governance practices. Consequently, trust may function more as a coping mechanism under uncertainty than as an informed assessment of digital risk.

Ethical Issues: Digital Exclusion and Algorithmic Dependency

Ethical debates surrounding digital health increasingly focus on exclusion, autonomy, and algorithmic dependency. Scholars warn that health systems may unintentionally deepen inequities when digital platforms become prerequisites for healthcare access. Patients unable to navigate digital systems risk exclusion from appointments, information access, monitoring programs, or preventive services.

For rural populations, digital exclusion intersects with economic precarity, infrastructural limitations, aging demographics, and educational inequality.

Research following the COVID-19 pandemic showed that rapid digitalization frequently assumed universal digital readiness that did not exist in practice (van Kessel et al., 2022). In some contexts, patients relied on family members or informal intermediaries to access digital healthcare services, raising additional privacy concerns.

Algorithmic dependency presents another emerging issue. As mHealth applications increasingly incorporate AI-driven recommendations, symptom prediction, and behavioral nudging, users may become dependent on systems they do not fully understand. While algorithmic guidance can improve efficiency and monitoring, it may also weaken critical judgment when users assume technological outputs are inherently objective or clinically validated.

This concern is particularly significant where health literacy is limited. Users with insufficient information literacy may struggle to distinguish evidence-based recommendations from commercially motivated engagement strategies. Moreover, algorithmic systems trained primarily on urban or majority-population datasets may inadequately represent rural populations, potentially generating biased or less accurate recommendations. Despite growing discussion of AI ethics in healthcare, relatively little research examines how algorithmic dependency operates under conditions of rural informational vulnerability.

Research Gaps and Theoretical Implications

The literature demonstrates substantial progress in understanding digital health adoption, literacy, and privacy governance individually. Yet significant fragmentation persists. Studies of health literacy rarely engage deeply with data governance frameworks. Privacy research often overlooks rural structural inequalities. Technology adoption models prioritize behavioral intention while underexamining constrained choice, institutional trust, and informational asymmetry.

Three major gaps emerge from this review. First, there is limited integration of information literacy and privacy governance within rural health decision-making research. Second, existing adoption models insufficiently explain why vulnerable populations continue using technologies they do not fully trust or understand. Third, empirical studies frequently measure digital access or usage without examining whether engagement leads to informed, autonomous, and privacy-aware decision-making.

This study addresses these gaps by conceptualizing privacy-aware mHealth engagement as a multidimensional process shaped simultaneously by literacy capacity, structural healthcare inequality, institutional trust, and governance visibility. Rather than treating digital adoption as inherently empowering, the study critically examines how rural users navigate health decisions under conditions of informational dependence and uneven privacy protection. In doing so, it contributes to emerging interdisciplinary debates on equitable digital health governance and the ethics of data-driven healthcare transformation.

4. Methodology

This study employed a convergent mixed-methods design integrating quantitative and qualitative

approaches to examine the relationship between information literacy, privacy awareness, and health decision-making among rural users of mobile health applications. The methodological framework was designed to capture both measurable behavioral patterns and the contextual realities shaping digital health engagement in underserved rural settings. A mixed-methods strategy was selected because the research problem extends beyond technological adoption and involves cognitive, ethical, and socio-institutional dimensions that cannot be adequately understood through a single methodological tradition. Recent digital health scholarship increasingly advocates methodological pluralism when studying vulnerable populations, particularly where digital trust, literacy, and governance intersect (Venkatesh et al., 2022; Creswell & Plano Clark, 2018). Quantitative methods allow examination of structural relationships among literacy, trust, and decision-making variables, while qualitative inquiry provides insight into how rural users interpret privacy risks, negotiate uncertainty, and make practical health choices under constrained healthcare conditions. The integration of these methods was therefore intended not only to strengthen validity through triangulation, but also to address limitations frequently observed in digital health research that relies exclusively on self-reported adoption metrics.

Research Design

The study adopted a convergent parallel mixed-methods design. Quantitative survey data, privacy audit findings, and app-level technical assessments were collected simultaneously with qualitative semi-structured interviews. Both strands were analyzed independently before integration during the interpretation phase. This design enabled the study to compare statistical patterns with lived experiences of rural users, thereby reducing interpretive reductionism. The quantitative component focused on modeling relationships between information literacy, privacy perception, digital trust, and health decision-making behavior. The qualitative component explored how participants interpreted app recommendations, understood privacy disclosures, and negotiated trade-offs between convenience and privacy risk. Combining these approaches was particularly important in rural contexts where digital practices are often shaped by social relationships, healthcare scarcity, and infrastructural limitations rather than purely individual preferences.

Study Population and Context

The target population consisted of adult rural residents who actively used at least one mobile health application for self-care, medication management, chronic disease monitoring, appointment scheduling, fitness tracking, or teleconsultation purposes. Participants were recruited from rural districts characterized by limited specialist healthcare access, moderate digital infrastructure, and increasing dependence on mobile internet connectivity for healthcare communication. The study focused specifically on rural populations because prior research demonstrates that rural users often experience simultaneous informational vulnerability and heightened dependence on digital health tools (Kim et al., 2022). Rural healthcare shortages may encourage reliance on mobile applications even where digital literacy and privacy awareness remain uneven. Consequently, rural populations provide an analytically significant context for examining tensions between technological access, trust, and informed health decision-making.

Eligibility criteria required participants to: be aged 18 years or older; reside in a rural or semi-rural locality for at least three years; use at least one mHealth application weekly; possess sufficient language proficiency to complete the survey or interview process. Participants with exclusively urban residence histories or no regular app usage were excluded to maintain contextual consistency.

Sampling Strategy

A stratified multistage sampling strategy was employed to improve representativeness across demographic and socioeconomic groups. Rural districts were first categorized according to healthcare accessibility, internet connectivity, and population density. Within each stratum, participants were recruited through local clinics, pharmacies, community health centers, and digital health outreach programs.
The quantitative sample consisted of 420 participants, a size considered appropriate for Structural Equation Modeling (SEM) based on recommendations for latent-variable analysis in health informatics research (Kline, 2023). Stratification ensured balanced representation across age, gender, educational attainment, and chronic disease status.

In addition to participant sampling, a purposive sample of commonly used mHealth applications was selected for technical privacy auditing. Apps were included if they:
had more than 50,000 downloads, targeted medication management, chronic disease monitoring, or telehealth services, were frequently identified by participants during survey screening.

A final set of 18 applications was analyzed to evaluate privacy architecture, permission requests, encryption practices, and third-party data-sharing behavior.

The qualitative component involved 32 semi-structured interviews selected from the survey participants using maximum variation sampling. This approach ensured inclusion of participants with differing literacy levels, ages, app usage patterns, and privacy attitudes. Interview recruitment continued until thematic saturation was achieved.

Data Collection Procedures

Information Literacy Survey

Information literacy was assessed using an adapted Digital Health Literacy Instrument (DHLI) combined with contextual rural-health indicators. The instrument

measured participants' abilities to: locate health information,evaluate credibility,interpret app-generated recommendations,understand privacy notifications,
compare conflicting digital health information. The survey utilized a five-point Likert scale ranging from "strongly disagree" to "strongly agree." Items were modified to reflect rural digital health realities, including limited provider access and reliance on non-clinical digital information sources. Pilot testing with 30 participants demonstrated acceptable internal consistency (Cronbach's alpha = .87). The adaptation of validated literacy instruments aligns with recommendations from recent rural eHealth studies emphasizing contextual calibration rather than direct urban-to-rural transferability (Neter & Brainin, 2022).

Health Decision-Making Behavior Assessment

Participants completed a behavioral assessment examining how mHealth applications influenced healthcare decisions. The instrument evaluated: reliance on app recommendations, medication adherence behaviors, consultation-seeking patterns, symptom interpretation, willingness to delay or seek clinical care based on app feedback.

Decision-making autonomy and perceived confidence were also measured. The behavioral framework was informed by health belief and technology acceptance research indicating that digital recommendations increasingly shape patient-level decision processes (Zhang et al., 2021).

Privacy Perception Questionnaire
Privacy perception was measured through a multidimensional questionnaire examining: trust in app providers, perceived transparency, awareness of data collection, concern regarding third-party sharing, perceived control over personal data, willingness to exchange privacy for healthcare convenience.

The instrument incorporated constructs from privacy calculus literature while adapting questions to rural healthcare dependency contexts. Rather than treating privacy concern as purely abstract, the questionnaire explored whether healthcare scarcity altered participants' tolerance toward data-sharing practices.

mHealth App Privacy Audit
A technical privacy audit was conducted on the selected applications using a structured assessment protocol adapted from prior mobile privacy research (Tangari et al., 2021). The audit evaluated:

requested permissions, encryption standards,privacy policy readability,third-party trackers,external data transmission behavior,consent architecture,account deletion mechanisms.
Network traffic monitoring and static permission analysis were conducted using Android testing environments and publicly available privacy inspection tools. Applications were scored according to transparency, proportionality of permissions, and data-sharing visibility.
This audit component was included because self-reported trust often diverges from actual technical privacy practices. Integrating technical analysis with user perception enabled examination of the gap between perceived and objective privacy protection.

Analytical Framework
Structural Equation Modeling (SEM)
SEM was employed to examine relationships among information literacy, privacy awareness, trust, and health decision-making behavior. SEM was selected because it enables simultaneous analysis of latent variables and indirect effects within complex sociotechnical systems.

The model hypothesized that: information literacy positively influences privacy awareness;
privacy awareness affects digital trust; digital trust mediates health decision-making behavior; objective privacy risk moderates trust formation. Model fit was assessed using Comparative Fit Index (CFI), Tucker–Lewis Index (TLI), Root Mean Square Error of Approximation (RMSEA), and Standardized Root Mean Square Residual (SRMR). Thresholds followed established methodological guidance for health informatics studies (Hair et al., 2022).

Regression Analysis
Multiple regression analysis examined predictors of privacy-aware decision-making, including age, education, app usage frequency, chronic illness status, and literacy levels. Hierarchical regression was used to isolate the explanatory contribution of privacy literacy beyond conventional demographic variables. Regression analysis was particularly important for identifying whether information literacy independently predicts privacy-sensitive behavior after controlling for socioeconomic differences.

Construction of the Information–Privacy Interaction Index (IPII)
To strengthen theoretical integration, the study developed an original composite metric termed the Information–Privacy Interaction Index (IPII). The index combined:

information literacy scores,
privacy awareness indicators,
behavioral autonomy measures,
objective app privacy risk scores.
The IPII was designed to measure the degree to which users can engage critically and autonomously with mHealth technologies under varying privacy conditions. Higher scores reflected stronger capacity for informed,

privacy-aware digital health engagement. The development of this index responds to limitations in prior literature where literacy and privacy are often measured independently despite their practical interdependence in real-world digital health environments.

Validity, Reliability, and Ethical Considerations

Several procedures enhanced methodological rigor. Survey instruments were pilot-tested and reviewed by specialists in public health, digital governance, and health informatics. Cronbach's alpha values above .80 indicated acceptable reliability across scales. Triangulation across surveys, interviews, and technical audits improved construct validity by reducing reliance on self-reported perceptions alone. Member-checking procedures were also used during qualitative analysis to ensure interpretive accuracy.

Ethical approval was obtained through institutional review procedures. Participants provided informed consent and were informed that no identifiable health information would be collected from their devices. Given the sensitivity of privacy-related discussions in rural communities, anonymization protocols were emphasized throughout data collection and reporting.

5. Results

The findings reveal that rural engagement with mobile health technologies is shaped by a complex interaction between information literacy, digital trust, perceived privacy protection, and healthcare necessity. Rather than functioning as isolated variables, these dimensions operated as interconnected mechanisms influencing how participants interpreted app-based health information, evaluated risk, and made practical healthcare decisions. Across all analytical stages, the results demonstrated that digital health adoption in rural populations cannot be adequately explained through access-based or technology-centered models alone. Instead, adoption patterns reflected broader structural conditions involving informational inequality, institutional trust, and constrained healthcare alternatives.

Information Literacy and Health Decision-Making Quality

Structural Equation Modeling (SEM) revealed a strong positive relationship between information literacy and health decision-making quality among rural users of mHealth applications. Participants with higher literacy scores demonstrated greater ability to critically interpret app-generated recommendations, compare digital information sources, and seek professional consultation when algorithmic outputs appeared uncertain or contradictory.

Importantly, decision-making quality was not measured merely through app usage frequency but through indicators of reflective engagement, including:

verification of symptom recommendations, awareness of app limitations, consultation-seeking behavior, cautious interpretation of automated alerts, ability to distinguish informational guidance from clinical diagnosis.

Higher-literacy participants were significantly less likely to engage in fully automated health decision-making. Instead, they tended to use mHealth applications as supplementary informational tools integrated into broader healthcare strategies. Interview findings reinforced this pattern. Participants with stronger digital literacy frequently described app recommendations as "guidance rather than authority," indicating a more balanced relationship between digital tools and clinical judgment.

Conversely, lower-literacy users showed greater dependence on app outputs, especially in contexts where local healthcare access was limited. Some participants described delaying clinical consultation after receiving reassuring app notifications, while others reported anxiety escalation due to symptom-checker interpretations they could not independently evaluate. These findings align with recent concerns in *The Lancet Digital Health* regarding algorithmic overreliance among digitally vulnerable populations (Kickbusch et al., 2021).

Regression analysis further demonstrated that information literacy remained a statistically significant predictor of health decision-making quality even after controlling for age, educational attainment, and frequency of app usage. This suggests that literacy functions not simply as a demographic characteristic but as an active interpretive capacity shaping digital health autonomy.

Privacy Perception and mHealth Adoption

Privacy perception influenced adoption behavior in nuanced and sometimes contradictory ways. Participants expressing high concern about data collection and third-party sharing were not necessarily less likely to use mHealth applications. Instead, privacy concern frequently coexisted with continued usage, particularly among individuals managing chronic health conditions.

This pattern reflected what interview participants often described as a "necessary compromise." Rural users facing limited provider availability, transportation barriers, or long appointment delays frequently perceived mHealth applications as indispensable despite uncertainty regarding privacy protections. As one participant explained during qualitative interviews, "I know they collect information, but I still need the app because the clinic is too far and appointments take weeks."

SEM results demonstrated that perceived usefulness partially moderated privacy concern.

Where participants believed applications substantially improved medication adherence, disease monitoring, or healthcare accessibility, privacy risk became secondary rather than irrelevant. However, this did not indicate genuine trust in data governance systems. Instead, many users described resignation or uncertainty regarding digital surveillance practices.

Notably, users rarely differentiated between different forms of privacy risk. Commercial advertising, behavioral tracking, geolocation collection, and third-party analytics were often interpreted as part of a generalized and unavoidable "digital exposure." This conceptual vagueness was more pronounced among lower-literacy participants, who frequently lacked familiarity with terms such as encryption, cloud storage, or data brokerage.

These findings complicate traditional privacy calculus models, which assume rational balancing between benefits and risks. In rural healthcare environments characterized by constrained alternatives, privacy decisions appeared less voluntary and more structurally conditioned.

The Gap Between Privacy Awareness and Actual App Behavior

One of the study's most significant findings emerged from comparison between self-reported privacy awareness and technical app audit results. Across all app categories, participants consistently underestimated the extent of data collection and third-party sharing occurring within the applications they trusted most. Technical privacy audits identified extensive permission requests among wellness and chronic disease applications, including:

location tracking,
contact access,
device identifiers,
behavioral analytics,
external advertising trackers.

Several applications transmitted user metadata to third-party services despite presenting simplified or reassuring privacy interfaces. Yet survey findings showed that many users interpreted visual professionalism, hospital affiliation, or high download counts as indicators of privacy safety. This disconnect was especially visible among users who reported "high confidence" in understanding app privacy practices while simultaneously failing to identify basic forms of passive data collection. The findings therefore revealed a substantial divergence between perceived privacy competence and objective governance awareness.

Wellness applications demonstrated the greatest disparity between user trust and technical privacy exposure. Participants generally perceived wellness apps as "low-risk" because they focused on exercise, diet, or sleep tracking rather than formal medical diagnosis. However, privacy audits showed that these apps frequently engaged in extensive behavioral tracking and third-party analytics integration. In contrast, telemedicine platforms demonstrated comparatively stronger encryption standards and clearer consent structures, likely due to closer institutional integration with regulated healthcare systems. Chronic disease management applications occupied an intermediate position: users often trusted them because of perceived medical legitimacy, yet technical analysis still revealed inconsistent transparency regarding data-sharing practices. These findings reinforce arguments from recent digital governance scholarship suggesting that privacy literacy cannot be reduced to subjective confidence alone (Morley et al., 2020). Effective privacy awareness requires not only understanding visible interfaces but also recognizing hidden data infrastructures operating beyond user perception.

High-Literacy Versus Low-Literacy Rural Users

Comparative analysis between high-literacy and low-literacy groups revealed substantial differences in digital health engagement patterns. High-literacy users demonstrated:

stronger skepticism toward automated recommendations,
greater likelihood of reviewing privacy policies,
more frequent use of secondary information verification,
increased preference for institutionally affiliated applications,
higher awareness of data-sharing risks.

These participants also exhibited more selective adoption behavior.

Rather than downloading multiple apps indiscriminately, they tended to prioritize applications linked to hospitals, pharmacies, or healthcare providers perceived as credible.

Low-literacy users, by contrast, often evaluated trustworthiness through superficial indicators such as interface simplicity, popularity rankings, or recommendations from peers and family members. While such relational trust mechanisms provided practical coping strategies, they also increased vulnerability to misleading or poorly governed platforms.

Importantly, low literacy did not correspond to technological passivity. Many low-literacy participants were highly active digital users. However, their engagement was more operational than interpretive. They could navigate interfaces efficiently while remaining uncertain about data governance implications or algorithmic reliability.

This distinction challenges assumptions that digital inequality primarily reflects lack of technological access. The findings instead support emerging theories of "critical digital inequality," where users may possess connectivity and technical familiarity yet still experience informational vulnerability due to limited evaluative capacity.

Trust as a Mediating Mechanism

Trust emerged as a central mediating variable linking information literacy to sustained mHealth adoption. SEM analysis showed that literacy indirectly influenced adoption behavior through its effect on institutional and technological trust.

However, the relationship was non-linear. Higher literacy increased awareness of privacy risk, which sometimes reduced unconditional trust in commercial applications. Yet this same awareness also strengthened

selective trust toward platforms perceived as transparent, clinically validated, or institutionally accountable.

In other words, literacy did not uniformly increase or decrease adoption. Instead, it transformed the basis upon which trust was constructed. High-literacy users engaged in more differentiated trust formation, whereas lower-literacy users often relied on generalized assumptions or necessity-driven acceptance. Across app categories, trust dynamics varied substantially:

Chronic disease applications generated the strongest long-term dependency because participants integrated them into ongoing medication and symptom management routines.

Telemedicine platforms benefited from institutional legitimacy and were associated with relatively higher confidence in privacy protection.

Wellness applications achieved rapid adoption but demonstrated weaker sustained trust due to perceived commercialization and inconsistent informational reliability.

These patterns suggest that trust in rural digital health environments is relational, contextual, and structurally mediated rather than purely technological. Trust often reflected broader experiences with healthcare accessibility, institutional reliability, and social vulnerability.

Overall, the results indicate that rural mHealth engagement cannot be understood solely through metrics of adoption or usability. The quality of digital health participation depends fundamentally on whether users possess the informational capacity, institutional support, and governance transparency necessary to make informed and privacy-aware health decisions. The findings therefore position information literacy not merely as a technical competency, but as a critical determinant of equitable digital health citizenship.

6. Discussion

The findings of this study show that rural mHealth engagement is not determined by access alone, but by the interaction of information literacy, trust formation, and privacy awareness. This aligns with digital health equity research arguing that digital transformation may widen disparities when tools are introduced without attention to social, infrastructural, and cognitive conditions of use. Richardson et al. describe "digital determinants of health" as factors that shape whether digital technologies reduce or reproduce inequality, including access, usability, literacy, and health-system integration. In this study, those determinants were visible not as abstract barriers, but as everyday decision-making pressures: rural users relied on apps because healthcare was distant, yet many lacked the literacy resources needed to evaluate app recommendations or data practices.

The relationship between information literacy and health decision-making quality confirms that literacy is not merely a supporting variable in digital health adoption. It is a condition for safe and autonomous engagement. High-literacy users treated mHealth outputs as provisional information, cross-checked recommendations, and were more likely to seek professional advice when app feedback appeared uncertain. Low-literacy users, by contrast, were more likely to interpret app outputs as authoritative, especially when clinical access was limited. This finding supports recent evidence that digital literacy can improve health behavior among rural older adults, but it also complicates such findings by showing that literacy must include privacy and algorithmic awareness, not only the ability to search for health information.

A central contribution of this study is its interpretation of rural vulnerability as both cognitive and structural. Rural users are not vulnerable simply because they lack skills. They become vulnerable when limited healthcare access, weak digital infrastructure, low transparency, and institutional dependency converge. This distinction is important because many digital health interventions still frame rural populations as "hard to reach" or "low adoption" groups. The results suggest a different problem: rural users may adopt mHealth tools actively, but under conditions of constrained choice. In this sense, adoption can conceal dependency. A patient may continue using a chronic disease app not because they fully trust it, but because it is the only practical tool available between clinic visits.

Privacy emerged as both a cognitive barrier and a structural barrier. Cognitively, many participants struggled to understand how apps collected, processed, and shared data. Structurally, even when participants expressed concern, they lacked realistic alternatives. This finding is consistent with JMIR research showing that patients are concerned about confidentiality, privacy, security, and regulatory oversight in mHealth systems, while also expecting developers to provide encryption, secure authentication, and regulatory compliance. However, the present study extends this evidence by showing that privacy concern does not necessarily reduce use among rural patients. Instead, privacy concern may coexist with continued adoption when health access is scarce.

This contradiction challenges privacy calculus theory. The traditional privacy calculus model assumes that users weigh risks and benefits rationally before disclosing data. In rural mHealth contexts, however, the "choice" to disclose may be shaped by necessity. Users may accept privacy risks because refusing them would mean losing access to medication reminders, teleconsultations, or symptom monitoring. Therefore, privacy behavior should not be read as consent in any strong ethical sense. It may reflect resignation, dependency, or lack of alternatives.

The gap between perceived privacy awareness and actual app behavior is particularly significant.

Participants often trusted apps because they looked professional, were recommended by others, or were associated with health-related branding. Yet technical audits revealed that many apps requested broad permissions or enabled third-party data flows. This mirrors prior evidence that mHealth apps may collect and share sensitive data in ways users do not fully

ejprd.org- Published by Riset Publishing Services LLC.

understand. Tangari et al.'s BMJ study found widespread privacy concerns across mobile health apps, including extensive data collection and third-party sharing practices. The present study confirms that this privacy gap is not only technical; it is interpretive. Users cannot meaningfully protect themselves from risks they cannot see.

Comparing app categories further clarifies the problem. Telemedicine platforms generated relatively higher trust because users associated them with healthcare institutions. Chronic disease apps created deeper dependency because they were embedded in daily self-management routines. Wellness applications, although perceived as less medically sensitive, often produced the greatest privacy ambiguity because users underestimated the value of behavioral data. This finding is policy-relevant because regulatory attention often focuses on explicitly medical data, while wellness and lifestyle data may also reveal health status through inference.

The ethical implications are substantial. Digital exclusion is no longer limited to lack of internet access. It now includes exclusion from meaningful consent, exclusion from understandable privacy choices, and exclusion from algorithmic accountability. If rural users must rely on apps whose data practices they cannot evaluate, then digital health risks shifting responsibility from institutions to individuals. This is ethically problematic because informed consent requires more than formal agreement. It requires comprehension, voluntariness, and realistic alternatives. Current consent mechanisms in mHealth environments often fail on all three grounds, especially for low-literacy users.

The study also contributes theoretically by proposing an integrated literacy–trust–privacy model. Existing adoption models such as TAM and UTAUT explain perceived usefulness, ease of use, and facilitating conditions, but they insufficiently account for privacy vulnerability and constrained healthcare choice. The present findings show that literacy influences trust, trust shapes adoption, and privacy awareness modifies the quality of health decision-making. Trust is therefore not a simple positive outcome. In some cases, trust enables appropriate engagement; in others, misplaced trust exposes users to hidden risks. This distinction strengthens digital health theory by moving beyond adoption as the primary indicator of success.

Policy implications follow directly from this interpretation. Rural digital health governance should not rely solely on expanding access or distributing apps. It should require privacy-by-design standards, plain-language consent, independent app certification, and rural-specific digital health literacy programs. The WHO's global digital health strategy emphasizes that digital health should support equitable and universal access to quality health services. To achieve that goal, rural implementation must include governance visibility: users should know who collects their data, why it is collected, where it goes, and how risks are controlled.

Finally, the findings suggest that rural mHealth policy should involve local healthcare intermediaries. Community health workers, rural clinicians, pharmacists, and local digital support staff can help translate privacy and health information into practical decision-making guidance. Without such support, mHealth may improve surface-level access while leaving deeper inequalities intact. Digital health equity therefore requires not only connectivity, but accountable systems that make informed, privacy-aware participation possible.

7. Limitations and Future Research

Several limitations should be considered when interpreting the findings of this study. First, although the research employed a stratified rural sampling strategy, the study remains shaped by regional and infrastructural specificities that may limit broader generalizability. Rural communities are not homogeneous environments; differences in internet connectivity, healthcare access, socioeconomic conditions, educational attainment, and local health governance can substantially influence digital health engagement. Consequently, the findings should not be interpreted as universally representative of all rural populations. The observed relationships between literacy, trust, and privacy awareness may manifest differently in regions with stronger public digital infrastructure, higher institutional trust, or alternative healthcare delivery systems.

Second, portions of the study relied on self-reported measures of information literacy, privacy awareness, and health decision-making behavior. Although validated instruments and triangulation procedures were used to improve reliability, self-reporting inevitably introduces interpretive and social desirability biases. Participants may overestimate their understanding of app privacy practices or underreport behaviors perceived as risky or uninformed. This limitation is particularly important in digital health research because confidence in technological understanding does not always correspond to actual evaluative competence. The divergence identified between perceived privacy awareness and technical app behavior suggests that subjective literacy and objective literacy may differ significantly.

Third, the technical privacy audit was necessarily limited in its capacity to fully examine backend data infrastructures. While the study assessed permissions, trackers, encryption visibility, and observable transmission behavior, it could not comprehensively verify proprietary server-side processing, algorithmic profiling systems, or undisclosed third-party data exchanges. Many commercial mHealth ecosystems operate through opaque architectures that remain inaccessible to independent researchers. As a result, the study likely captures only part of the broader data governance landscape influencing user privacy exposure.

Another limitation concerns the rapidly evolving nature of mobile health technologies. mHealth applications

frequently update interfaces, consent structures, tracking mechanisms, and data-sharing arrangements. Regulatory standards also continue to evolve in response to emerging concerns regarding AI, digital surveillance, and platform accountability. Consequently, the governance conditions analyzed in this study should be understood as temporally situated rather than permanently stable. Findings regarding app behavior and privacy transparency may therefore shift over time as technologies and regulations develop.
Future research should expand beyond static assessments of literacy and adoption toward more adaptive and context-sensitive approaches. One promising direction involves the development of AI-assisted rural health literacy assessment tools capable of identifying literacy vulnerabilities in real time and tailoring educational support accordingly. Such systems could potentially help bridge gaps between technical functionality and meaningful understanding, particularly for aging or medically vulnerable populations.
Comparative cross-country studies would also be valuable for examining how rural digital health experiences differ across regulatory systems, healthcare infrastructures, and cultural environments. Current digital health scholarship remains disproportionately centered on high-income or urban contexts. Comparative rural analyses could reveal how governance models, institutional trust, and digital inequality interact under different sociopolitical conditions.

Longitudinal research is similarly needed to examine how trust and privacy awareness evolve over time.
Digital trust is unlikely to remain static; it may strengthen, weaken, or fragment in response to personal experiences, media coverage, policy changes, or data breach events. Longitudinal designs would therefore provide deeper insight into the temporal dynamics of privacy perception and digital dependency.

Finally, future studies should integrate behavioral analytics alongside self-reported measures. Combining qualitative interviews with anonymized interaction data, usage logs, or decision-pattern analysis could improve understanding of how users actually engage with mHealth systems in everyday settings. Such approaches may help address the growing gap between what users believe they understand about digital health technologies and how those technologies function operationally within broader data ecosystems.

8. Conclusion

This study examined the relationship between information literacy, privacy perception, digital trust, and health decision-making among rural users of mobile health applications. The findings demonstrate that mHealth adoption in rural contexts cannot be understood solely through technological access or usability metrics. Instead, digital health engagement emerges through a complex interaction of informational capability, healthcare dependency, institutional trust, and uneven visibility into data governance practices.

The study found that higher levels of information literacy were associated with more reflective and autonomous health decision-making. Rural users with stronger literacy capacities were better able to evaluate app-generated recommendations, question automated outputs, and integrate digital information into broader healthcare strategies. By contrast, lower-literacy users were more likely to rely on app recommendations without critically assessing their reliability or privacy implications, particularly where healthcare alternatives were limited. These findings reinforce the argument that digital participation alone does not guarantee informed or equitable healthcare engagement.
A second major contribution concerns the role of privacy within rural mHealth ecosystems. Privacy was not experienced merely as a technical issue, but as both a cognitive and structural challenge. Many participants expressed concern regarding data collection and third-party sharing while simultaneously continuing to use applications because they perceived few realistic alternatives. The study therefore highlights a critical tension within contemporary digital health systems: populations most dependent on mHealth technologies may also be among the least equipped to evaluate associated privacy risks. This creates a form of digital vulnerability rooted not only in technological inequality, but also in informational asymmetry and constrained healthcare choice.
The findings additionally revealed a substantial gap between perceived privacy awareness and actual app behavior. Technical audits demonstrated that several widely trusted applications engaged in extensive data collection and tracking practices that users neither expected nor fully understood. Trust frequently relied on interface familiarity, institutional branding, or perceived medical legitimacy rather than objective governance transparency. This suggests that digital trust in rural settings often functions as a practical necessity under conditions of healthcare scarcity rather than as evidence of informed confidence in data protection systems.

The study offers several policy implications. For policymakers, expanding rural digital health infrastructure must be accompanied by enforceable governance frameworks emphasizing transparency, accountability, and privacy-by-design standards. Regulatory systems should require simplified consent mechanisms, clearer disclosure of third-party data sharing, and independent oversight of commercial mHealth applications. Rural digital health policy should also recognize information literacy as a public health priority rather than a purely educational concern.
For app developers, the findings underscore the importance of designing applications that support meaningful understanding rather than passive acceptance. Privacy notices should be accessible, context-sensitive, and understandable for users with varying literacy levels. Developers should minimize unnecessary data collection, improve transparency regarding algorithmic recommendations, and incorporate user-centered ethical safeguards into platform architecture.

Healthcare systems likewise have an essential role in reducing rural digital vulnerability. Clinicians, pharmacists, and community health workers can function as trusted intermediaries who help patients interpret digital information and understand privacy implications.

Integrating digital literacy support into routine healthcare delivery may improve not only app usage quality but also long-term patient autonomy and trust. Ultimately, equitable digital health governance requires moving beyond narrow models of technological adoption toward frameworks that prioritize informed participation, transparency, and social accountability. As health systems worldwide increasingly depend on mobile and data-driven technologies, the challenge is no longer simply connecting rural populations to digital tools. The deeper challenge lies in ensuring that digital transformation does not reproduce existing inequalities under the language of innovation. Future global health strategies must therefore treat information literacy, privacy protection, and ethical governance as foundational conditions for sustainable and equitable digital healthcare systems.

References

1. Aji, M., Ismail, M., Rahman
2. , F., & Yusuf, H. (2023). Factors influencing telehealth adoption in underserved populations. *NPJ Digital Medicine, 6*(1), 88–101. https://doi.org/10.1038/s41746-023-0088-1
3. Campos-Castillo, C., & Anthony, D. (2021). Racial and rural disparities in self-reported telehealth use during the COVID-19 pandemic. *Journal of the American Medical Informatics Association, 28*(1), 190–195. https://doi.org/10.1093/jamia/ocaa221
4. Cohen, I. G., & Mello, M. M. (2020). HIPAA and protecting health information in the 21st century. *JAMA, 323*(3), 231–232. https://doi.org/10.1001/jama.2019.18548
5. Coughlin, S. S., Vernon, M., Hatzigeorgiou, C., & George, V. (2020). Health literacy, social determinants of health, and disease prevention and control. *Journal of Environment and Health Sciences, 6*(1), 3061–3072. https://doi.org/10.15436/2378-6841.20.3061
6. Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE.
7. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008
8. de Figueirêdo, R. C., et al. (2024). Preparation and validation of the instrument "QualiAPS digital-Brazil". *Frontiers in Public Health, 12*, 1304148. https://doi.org/10.3389/fpubh.2024.1304148
9. Duong, J. B., Chen, A., & Martinez, R. (2025). Caregiver perceptions of healthcare barriers. *NPJ Digital Medicine, 8*(1), 213–227. https://doi.org/10.1038/s41746-025-02131-x
10. Fan, S., Jain, R. C., & Kankanhalli, M. S. (2023). Factors affecting willingness to use mHealth apps. *NPJ Digital Medicine, 6*(1), 147–160. https://doi.org/10.1038/s41746-023-00891-2
11. Federal Trade Commission. (2024). FTC finalizes changes to the Health Breach Notification Rule.
12. Farai, O. A., et al. (2024). Digital health technologies in chronic disease management. *International Journal of Research and Scientific Innovation, 10*(12), 533–551.
13. Grundy, Q., et al. (2019). Data sharing practices of medicines related apps. *BMJ, 364*, l920. https://doi.org/10.1136/bmj.l920
14. Hair, J. F., et al. (2022). *A primer on PLS-SEM* (3rd ed.). SAGE.
15. Hoque, R., & Sorwar, G. (2019). Adoption of mHealth by older adults. *International Journal of Medical Informatics, 101*, 75–84. https://doi.org/10.1016/j.ijmedinf.2017.02.002
16. Hu, S., Zhang, Y., & Liang, M. (2025). Digital health: Applications and challenges. *NPJ Digital Medicine, 8*(1), 54–71. https://doi.org/10.1038/s41746-025-01154-6
17. Iwaya, L. H., Ahmad, A., & Babar, M. A. (2020). Security and privacy for mHealth systems. *IEEE Access, 8*, 150081–150112.
18. Jat, M., Sharma, P., & Kaur, H. (2025). Digital health interventions in low-resource settings. *JMIR Formative Research, 9*, e69824.
19. Kickbusch, I., et al. (2021). Digital health literacy and health equity. *The Lancet Digital Health, 3*(9), e545–e547.
20. Kim, H., Xie, B., & Wahbeh, H. (2022). Mobile health adoption in rural populations. *JMIR mHealth and uHealth, 10*(4), e34875.
21. Kline, R. B. (2023). *Principles and practice of SEM* (5th ed.). Guilford Press.
22. Kokolakis, S. (2017). Privacy paradox phenomenon. *Computers & Security, 64*, 122–134.
23. Levy, H., et al. (2023). Digital health literacy among rural populations. *BMC Digital Health, 1*(1), 15–29.
24. Lestari, H. M., et al. (2024). Barriers to telemedicine adoption. *Clinical Epidemiology and Global Health*.
25. Manyazewal, T., et al. (2021). Digital health technologies in Ethiopia. *NPJ Digital Medicine, 4*(1), 125.
26. Monteiro, V. C. M., et al. (2025). Digital health in primary care. *BMC Primary Care, 26*(1), 44–58.
27. Morley, J., et al. (2020). Ethical guidelines for COVID-19 tracing apps. *The Lancet Digital Health, 2*(7), e329–e330.
28. Morris, B. B., et al. (2021). Digital health in rural cancer care. *Journal of Rural Health, 38*(3), 493–511.
29. Neter, E., & Brainin, E. (2022). eHealth literacy in rural communities. *Health Communication, 37*(5), 612–620.
30. Obar, J. A., & Oeldorf-Hirsch, A. (2020). Privacy policies and informed consent. *Information, Communication & Society, 23*(1), 128–147.

31. Richardson, S., et al. (2022). Framework for digital health equity. *NPJ Digital Medicine, 5*(1), 119.
32. Richardson, S., et al. (2023). Digital determinants of health. *NPJ Digital Medicine, 6*(1), 42–56.
33. Riccalton, V., et al. (2026). mHealth applications systematic review protocol. *JMIR Research Protocols, 15*, e72664.
34. Silva, C. R. D. V., et al. (2022). Digital health in primary care (COVID-19). *JMIR Human Factors, 9*(2), e35380.
35. Silva, Í. S., et al. (2024). Digital health and quality of care. *Frontiers in Public Health, 12*, 1443862.
36. Sørensen, K., et al. (2021). Health literacy in the digital age. *Health Promotion International, 36*(Suppl. 1), i1–i14.
37. Tangari, G., et al. (2021). Mobile health and privacy. *BMJ, 373*, n1248.
38. U.S. Department of Health and Human Services. (2024). Online tracking technologies and HIPAA.
39. van Kessel, R., et al. (2022). Digital health inequalities during COVID-19. *JMIR, 24*(2), e34453.
40. Venkatesh, V., et al. (2022). Technology adoption in healthcare. *MIS Quarterly, 46*(2), 875–910.
41. Weinhold, I., & Gurtner, S. (2014). Rural healthcare shortages. *Health Policy, 118*(2), 201–214.
42. Western, M. J., et al. (2025). Digital health divide. *Digital Health, 11*, 1–18.
43. World Health Organization. (2021). *Global strategy on digital health 2020–2025*.
44. Zaghloul, H., et al. (2025). Digital health literacy in chronic diseases. *JMIR, 27*, e56231.
45. Zhang, X., et al. (2021). mHealth adoption and gender differences. *Telemedicine and e-Health, 27*(3), 301–311.
46. Zhao, Y., Ni, Q., & Zhou, R. (2020). mHealth adoption meta-analysis. *International Journal of Information Management, 43*, 342–350.
47. Zhou, L., et al. (2019). mHealth app usability questionnaire (MAUQ). *JMIR mHealth and uHealth, 7*(4), e11500.