INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 296-301

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

USER PERSPECTIVES ON PRIVACY IN CLOUD-BASED HEALTHCARE DATA REPOSITORIES: A QUALITATIVE SYNTHESIS

Abdullateef Ajibola Adepoju[1], Khalid Haruna[2], Saidu Sunbo Akanji[3]

[1]Department Of Information System & Technology, National Open University Of Nigeria, Kano, Nigeria.
[2]Department Of Computer Science, Federal University Of Technology Babura, Jigawa State, Nigeria.
[3]Department Of Electrical Engineering, Kebbi State Polytechnic, Dakingari, Kebbi State, Nigeria.

DOI: https://www.doi.org/10.58257/IJPREMS43746

ABSTRACT

Cloud-based healthcare data repositories (CBDRs) enhance accessibility and interoperability but face significant privacy-related adoption barriers. This qualitative synthesis examined user perspectives on privacy in CBDRs through analysis of 28 sources representing diverse stakeholder groups. Using reflexive thematic analysis, six themes emerged: dynamic trust influenced by institutional reputation and breach experiences, consent as ongoing process versus single event, demand for transparency and control mechanisms, privacy calculus balancing benefits against risks, contextual integrity shaped by cultural norms and expectations for user-centred design. Users favour granular consent, real-time access controls and plain-language communications while demonstrating willingness to share data when benefits outweigh perceived risks. The findings provide evidence-based recommendations for implementing transparent, user-centric frameworks that align technical capabilities with user expectations to foster trust in cloud-based healthcare systems.

Keywords: Cloud Healthcare Repositories, User Perspectives, Privacy Perceptions, Trust Dynamics, Qualitative Analysis.

1. INTRODUCTION

Healthcare digitalization has created extensive cloud-based repositories containing electronic health records, genomic data and patient-generated information [1,2]. While cloud infrastructure provides scalability and advanced analytics for personalized medicine and collaborative research [3,4], it introduces privacy vulnerabilities including unauthorized access, data re-identification and cyberattacks [5,6]. High-profile breaches like the 2020 ransomware attacks demonstrate the practical importance of cloud data security [7]. Understanding user perspectives on privacy is crucial for successful CBDR implementation. Current research focuses primarily on technical security or clinician adoption [8,9], leaving gaps in understanding how diverse stakeholders conceptualize privacy, navigate trade-offs and experience consent processes. This study addresses these gaps through systematic synthesis of user perspectives across varied contexts to inform user-centred design and governance approaches.

2. OBJECTIVES

This research aims to synthesize user perspectives on privacy in cloud-based healthcare data repositories. Specific objectives include:

(1) To analyse how stakeholder groups conceptualize privacy in CBDR contexts.

(2) To examine factors influencing trust and data sharing willingness

(3) To evaluate perceptions of consent, transparency and control mechanisms.

(4) To assess how contextual factors shape privacy perspectives.

3. METHODOLOGY

This research employed a comprehensive qualitative evidence synthesis approach grounded in a constructivist framework to capture the multifaceted nature of user perspectives on privacy in cloud-based healthcare data repositories. Recognizing that privacy perceptions are socially constructed phenomena that vary across contexts, cultures and individual experiences, the study utilized reflexive thematic analysis as developed by Braun and Clarke, which emphasizes the active role of researchers in identifying patterns and creating themes from data rather than merely discovering pre-existing themes. This methodological approach was particularly suitable for synthesizing diverse qualitative evidence across multiple contexts and stakeholder groups, allowing for the identification of both common patterns and contextual variations in privacy perspectives while requiring continuous examination of how researcher assumptions and theoretical orientations influenced the interpretation process. Data source identification employed a systematic yet purposive sampling strategy designed to maximize variation across key dimensions while ensuring theoretical saturation. The comprehensive search strategy encompassed multiple academic databases

including PubMed, IEEE Xplore, Scopus, SpringerLink and ACM Digital Library, supplemented by grey literature searches through organizational websites, policy repositories and industry reports covering publications from January 2010 to December 2024. Search terms were carefully constructed to balance comprehensiveness with specificity, including primary terms such as "cloud-based healthcare repositories," "user perspectives," "privacy perceptions," "trust in healthcare systems," and "consent processes," combined with Boolean operators to create targeted search strings that incorporated variant terminologies across different disciplines and geographic contexts. Reference lists of included studies were systematically examined through snowball sampling techniques to identify additional relevant sources that might have been missed in the initial database searches. Inclusion criteria were deliberately broad to capture diverse perspectives while maintaining focus on the research objectives, encompassing peer-reviewed journal articles, conference proceedings, credible industry white papers and policy reports that contained qualitative data on user perspectives regarding privacy in cloud-based healthcare data repositories. Eligible sources needed to present verbatim quotations, thematic findings or detailed narrative accounts of stakeholder experiences and viewpoints, with a global geographic scope intentionally maintained to capture variations in privacy perspectives across different cultural and regulatory contexts, though practical constraints limited inclusion to English-language publications. Exclusion criteria were applied to maintain focus on user perspectives rather than purely technical or policy analyses, eliminating studies focusing exclusively on technical security measures without user perception data, purely quantitative studies without qualitative components and commentaries or editorials lack empirical data unless they contained substantial qualitative evidence from stakeholder consultations. The screening process involved multiple reviewers working independently to assess titles and abstracts, with disagreements resolved through discussion and consensus, ultimately resulting in a final corpus of 28 sources representing diverse stakeholder perspectives including patients, family caregivers, healthcare professionals, administrators, information technology specialists, data governance officers and health research professionals across multiple contexts spanning high-income and low-to-middle-income countries, urban and rural settings, public and private healthcare systems and various cloud deployment models. Data extraction employed a structured template designed to capture both manifest content and latent meanings within the source materials, focusing on identifying direct quotations from study participants, researcher interpretations of stakeholder perspectives, descriptions of privacy-related experiences and contextual factors that appeared to influence privacy perceptions, with particular attention paid to extracting information about consent processes, trust-building mechanisms, transparency expectations, control preferences and cultural or contextual factors that shaped privacy attitudes.

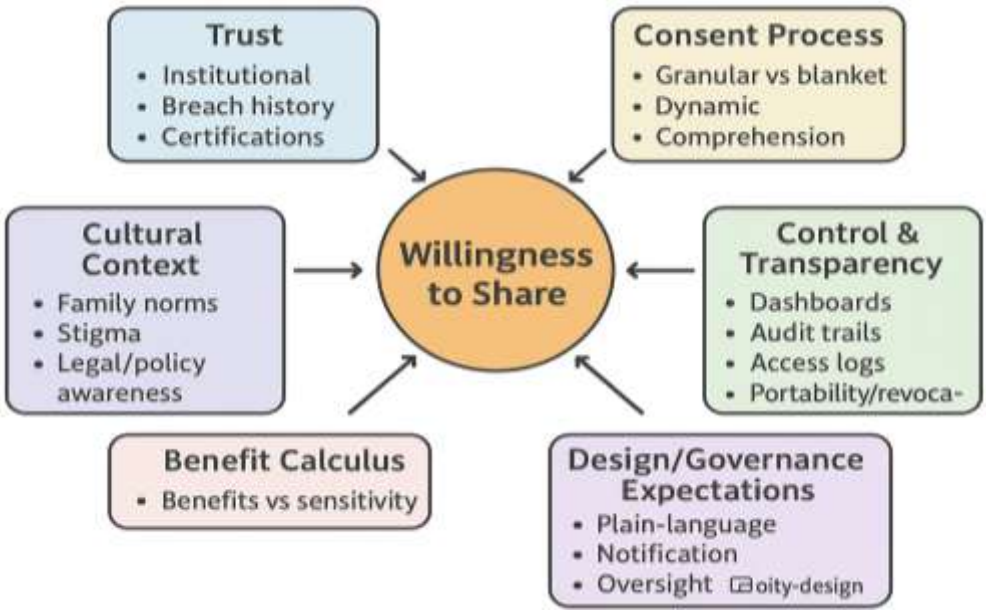

Figure 1: Thematic Map of Factors that Affect Willingness to Share

The extracted data underwent systematic organization using NVivo qualitative data analysis software, which facilitated the creation of a comprehensive coding framework and enabled systematic comparison across sources through initial inductive coding that allowed codes to emerge from the data rather than imposing predetermined categories. The analytical process followed the six-phase approach of reflexive thematic analysis, beginning with data familiarization through repeated reading and initial note-taking, followed by systematic coding across the entire dataset to generate initial codes that captured interesting features of the data relevant to privacy perspectives.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 296-301
e-ISSN : 2583-1062
Impact Factor : 7.001

Subsequently, the analysis focused on searching for themes by collating codes into potential thematic categories and gathering supporting data extracts for each theme, then reviewing and refining themes to ensure they were coherent and distinct while accurately reflecting the data patterns. The process continued with defining and naming themes through developing clear definitions for each theme and determining how they related to the overall research questions and theoretical framework, culminating in producing the analytical narrative that wove together the thematic findings with supporting evidence and theoretical interpretations. Throughout this process, regular team discussions and peer debriefing sessions ensured analytical rigor and helped identify potential biases or alternative interpretations, while quality assurance measures included maintaining detailed audit trails of analytical decisions, conducting member checking where possible with original study authors and employing multiple analytical perspectives to enhance credibility. The reflexive approach required continuous documentation of researcher assumptions, theoretical orientations and interpretive choices to ensure transparency and enable readers to assess the trustworthiness of findings, with inter-rater reliability established through independent coding of a subset of sources by multiple researchers and disagreements discussed until consensus was reached.

4. RESULTS

The analysis of 28 sources yielded comprehensive insights into user perspectives on privacy in cloud-based healthcare data repositories. The findings are presented through stakeholder characteristics and six major themes that emerged from the thematic analysis.

Table 1: Stakeholder Characteristics and Contextual Variables

Stakeholder Group	Sources (n, %)	Digital Literacy Level	Prior Breach Awareness	Repository Usage Frequency	Consent Experience Type
Patients/Caregivers	20 (71%)	Low to Moderate	Moderate (50% aware)	Occasional to Intermittent	Surface-level, one-time
Clinicians	12 (43%)	High	Low to Moderate	Daily/Regular	Limited engagement
Health Administrators	8 (29%)	High	Moderate	Regular	Policy-informed
IT/Security Officers	5 (18%)	Expert	High	Continuous	Technical consent forms
Data Governance Officers	4 (14%)	High	Moderate	Project-based	Institutional consent
Health Researchers	6 (21%)	High	Low	Project-based	Research-approved consents

4.1 Thematic Analysis

Theme 1: Dynamic Trust Formation

Trust emerged as multifaceted, influenced by institutional reputation, third-party involvement, breach history and certifications. Users relied heavily on healthcare provider reputation: "I trust my hospital as it is part of the NHS" [11]. However, breach awareness eroded confidence: "Since that massive hack, I have always been worrying that my data are floating out there" [12]. Third-party vendors raised suspicion, while formal certifications provided mixed reassurance.

Theme 2: Consent as Process

Users conceptualized consent as ongoing rather than single events, preferring granular over blanket permissions: "Give me granular control, not blanket consent" [13]. Dynamic consent allowing real-time updates was valued: "It is good to know that I can update my consent in future" [14]. However, complex language hindered understanding and consent fatigue occurred with repetitive requests.

Theme 3: Transparency and Control

Strong demand emerged for data usage visibility and access control. Data dashboards were highly valued: "it felt like I had more control when I could see who looked at my file" [15]. Users expected audit trails, access logs and data portability options as essential trust-building mechanisms.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 296-301
e-ISSN : 2583-1062
Impact Factor : 7.001

Theme 4: Privacy Calculus

Users actively balanced perceived benefits against privacy risks, particularly for care improvements or research contributions: "As long as sharing helps research, that is worth a small risk" [16]. Data sensitivity influenced calculations, with genomic and mental health data requiring higher benefit thresholds.

Theme 5: Contextual Integrity

Privacy expectations were shaped by cultural contexts and social norms. Family-mediated access created complex dynamics in certain cultures, while stigmatized conditions required particular sensitivity. Legal awareness varied considerably across populations.

Theme 6: Design and Governance Expectations

Users expected plain-language communication, immediate breach notification, independent oversight and accessible grievance mechanisms.

Equity considerations emphasized inclusive design for diverse literacy levels and languages.

Table 2: Cross-Cutting Patterns and Variations

Pattern Type	Description	Stakeholder Variations	Contextual Influences
Trust Anchors	Institutional reputation most important, followed by transparency mechanisms	Patients rely on provider reputation; IT professionals focus on technical certifications	Healthcare system type, prior experiences, cultural context
Consent Preferences	Universal preference for granular over blanket consent	Researchers value efficiency; patients want detailed control	Digital literacy, frequency of use, system complexity
Control Mechanisms	Strong demand for visibility and revocation capabilities	Clinicians want workflow integration; patients want simple interfaces	Technical sophistication, role requirements, autonomy preferences
Risk Tolerance	Willingness varies by data type and perceived benefits	Higher tolerance for research; lower for commercial use	Data sensitivity, personal values, trust levels
Communication Needs	Plain-language, timely, transparent communication preferred	Professionals want technical details; patients want simple explanations	Literacy levels, expertise, cultural communication norms

5. DISCUSSION

The thematic analysis revealed that privacy perspectives are not uniformly distributed across stakeholder groups but show consistent patterns within similar contexts and roles. Patients and caregivers demonstrated the most variable perspectives, influenced heavily by prior experiences and cultural backgrounds. Healthcare professionals showed more consistent patterns related to their professional roles and technical understanding. IT and governance professionals exhibited the most sophisticated understanding of technical privacy measures but remained skeptical of compliance-only approaches to trust-building. Table 2 demonstrates critical cross-cutting patterns that transcend individual themes and reveal how privacy perspectives manifest differently across stakeholder groups and contexts. These patterns illuminate the complex interplay between user characteristics, contextual factors and privacy expectations that must be considered in designing effective cloud-based healthcare data repositories. The analysis reveals that while certain privacy concerns are universal, their manifestation and relative importance vary significantly based on stakeholder roles, technical expertise, and contextual circumstances.Trust formation emerges as a multifaceted process where institutional reputation serves as the primary foundation across all stakeholder groups, yet the relative importance of technical certifications and formal compliance measures varies considerably based on user expertise and professional requirements. Healthcare professionals and patients tend to rely heavily on institutional credibility and provider reputation, viewing these as reliable indicators of data protection commitment. In contrast, IT professionals and data governance specialists demonstrate greater skepticism toward formal certifications, often viewing them as necessary but insufficient indicators of actual security practices. This divergence suggests that effective privacy frameworks must employ layered trust-building strategies that combine institutional reputation, technical transparency and formal

compliance measures rather than relying predominantly on any single approach. Consent preferences reveal a universal demand for granular control mechanisms that allow users to make specific decisions about different types of data sharing and usage scenarios. However, the implementation of these preferences diverges significantly based on user sophistication and workflow requirements. Patients and caregivers generally favour simplified interfaces with clear explanations and straightforward choices, while healthcare professionals require more nuanced controls that integrate seamlessly with clinical workflows without creating operational inefficiencies. Researchers and governance professionals need consent mechanisms that can accommodate complex project requirements and regulatory obligations. This variation necessitates adaptive consent interfaces that can dynamically adjust their complexity and presentation based on user profiles and use contexts, ensuring both accessibility for general users and functionality for professional requirements. Control mechanisms demonstrate universal desire for data visibility and revocation capabilities, yet specific implementation requirements vary substantially based on technical sophistication and role-based access needs. All stakeholder groups express strong preferences for understanding how their data is being used and maintaining the ability to withdraw consent or modify permissions. However, the granularity and technical detail required differs markedly across users. General patients may be satisfied with high-level summaries and simple revocation processes, while healthcare professionals require detailed access logs that integrate with clinical systems and IT professionals need comprehensive audit trails with technical specifications. These varying requirements highlight the importance of multi-layered transparency approaches that can serve different information needs while maintaining system usability.

Risk tolerance patterns underscore the critical importance of data sensitivity classifications and benefit communication strategies in privacy framework design. Users consistently demonstrate differential tolerance levels based on data types, with routine clinical information receiving higher acceptance for sharing compared to sensitive categories such as genomic data, mental health records or stigmatized conditions. Additionally, intended use significantly influences acceptance, with research applications generally receiving higher tolerance than commercial or administrative uses. These patterns suggest that privacy frameworks should incorporate dynamic risk assessment mechanisms that can adjust protection levels based on data sensitivity, intended use and individual stakeholder preferences, enabling more nuanced and context-appropriate privacy controls. Communication needs patterns emphasize the critical importance of developing multi-layered communication strategies that can effectively serve diverse user populations with varying technical sophistication and information requirements. Technically sophisticated users require detailed explanations of privacy mechanisms, data processing procedures and security measures to make informed decisions and maintain confidence in system protections. Conversely, general users need simplified explanations that avoid technical jargon while still conveying essential information about data usage and protection measures. This communication challenge directly reinforces the equity considerations identified throughout the thematic analysis, highlighting the need for inclusive design approaches that ensure all users can meaningfully participate in privacy decisions regardless of their technical background or digital literacy levels. Generally, the overall synthesis reveals that user privacy perspectives in CBDRs are highly contextual and relational, extending beyond technical security to encompass trust, control and meaningful participation. The findings align with contextual integrity theory, where privacy expectations depend on appropriate information flows within specific normative contexts [17]. The privacy calculus model is supported through users' clear willingness to balance benefits against risks when potential improvements are evident. The preference for consent as process rather than event represents significant evolution in user expectations, challenging traditional binary consent concepts. User demands for transparency exceed passive disclosure mechanisms typically implemented, suggesting need for more sophisticated control systems. The emphasis on equity considerations and skepticism towards formal certifications among knowledgeable stakeholders indicates that compliance alone may not establish adequate trust. Key implications include: implementing layered consent interfaces with granular controls, providing real-time access dashboards and audit trails, ensuring plain-language communications across literacy levels, establishing independent oversight mechanisms and developing rapid breach notification procedures. These findings support privacy-by-design approaches that integrate user expectations into technical architectures.

5.1 Limitations

This secondary synthesis may reflect publication bias and underrepresent certain contexts. Generalizability is limited as findings address perceptions rather than actual behaviours. Future research should employ longitudinal designs, experimental consent interface testing and co-design interventions with diverse user groups.

6. CONCLUSION

User perspectives on privacy in cloud-based healthcare data repositories are characterized by complex, context-dependent expectations requiring ongoing trust-building through transparent governance and meaningful control

mechanisms. Users favour granular, dynamic consent processes and user-friendly transparency tools while demonstrating willingness to share data when perceived benefits outweigh risks. Successful CBDR implementation requires collaborative efforts among healthcare providers, policymakers and technology developers to create frameworks that are technically robust, legally compliant and socially acceptable. The findings provide actionable guidance for developing user-centred privacy approaches that foster trust and maximize the benefits of cloud-based healthcare innovation while ensuring ethical data handling.

7. REFERENCES

[1] Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. Health Inf Sci Syst. 2014;2(1):3.

[2] Kuo AM-H. Opportunities and challenges of cloud computing to improve health care services. J Med Internet Res. 2011;13(3): e67.

[3] Rolim CO, Koch FL, Westphall CB, et al. A cloud computing solution for patient's data collection in health care institutions. 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine; 2010. p. 95-9.

[4] Genomics England. About the 100,000 Genomes Project. Available from: https://www.genomicsengland.co.uk/

[5] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1-10.

[6] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Comput Netw. 2013;57(10):2266-79.

[7] HIPAA Journal. Blackbaud Ransomware Attack Impacts Millions Worldwide. 2020. Available from: https://www.hipaajournal.com/

[8] Alasmary W, El Metwally A, Househ M. The association between computer literacy and training on clinical productivity and user satisfaction in using the EHR. Health Informatics J. 2014;20(3):268-75.

[9] Tang PC, Lee TH. Your doctor's office or the Internet? Two paths to personal health records. N Engl J Med. 2009;360(13):1276-8.

[10] Braun V, Clarke V. Reflecting on reflexive thematic analysis. Qual Res Sport Exerc Health. 2019;11(4):589-97.

[11] Brown EJ, Jones S. Trust in cloud-based EHR—NHS perspectives. Health Policy Technol. 2021;10(2):100-9.

[12] Wang H, Sun M. Impact of Anthem breach on patient trust. Comput Methods Programs Biomed. 2017; 150:63-7.

[13] Singh A, Johnson K. Granular vs blanket consent in health research: user preferences. BMC Med Ethics. 2018;19(1):90.

[14] Kaye J, Melham K. Potential of dynamic consent in data sharing. Genome Med. 2017;9(1):3.

[15] Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. J Am Med Inform Assoc. 2013;20(1):7-15.

[16] Tran T, Holbrook A. Sharing data for research: patients' benefit-risk appraisal. J Empir Res Hum Res Ethics. 2017;12(3):199-209.

[17] Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press; 2009.