Evaluating User Perceptions of Privacy Protection in Smart Healthcare Services

Huan Gua, Elias Seid, Yuhong Li, Fredrik Blix
Department of Computer and Systems Sciences
Stockholm University, Sweden
E-mail: (Huan, elias.seid, Yuhong, Fredrik) @dsv.su.se

***Abstract*—As smart healthcare services rapidly evolve, ensuring user privacy has become a critical concern. While prior research has focused extensively on technical solutions, the user perspective on privacy protection remains underexplored. This study addresses that gap by examining how users perceive both technical and organizational privacy protection measures across four smart healthcare service types: wearable devices, mobile health apps, telehealth platforms, and medicine delivery systems. Through a qualitative survey, the study uncovers a duality in user perceptions. Positive perceptions relate to multi-layer technical safeguards, regulatory oversight such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and proactive provider practices, such as transparent privacy policies and breach responses. On the other hand, negative perceptions center on lack of transparency, limited user control, forced consent to privacy terms, and both cognitive and operational barriers to engaging with privacy features. These findings reveal a critical imbalance in user-provider power dynamics and call for user-centric privacy strategies that balance protection with usability. The study contributes to theoretical advancements in privacy calculus, Technology Acceptance Model (TAM), and Unified Theory of Acceptance and Use of Technology (UTAUT) by refining constructs, such as perceived control, facilitating conditions, and transparency. Practical recommendations are offered to guide more inclusive, adaptable, and empowering privacy solutions in smart healthcare contexts.**

Keywords-privacy protection measures; privacy-preserving techniques; smart healthcare; users' perception.

I. INTRODUCTION

Smart cities embody the integration of digital technologies into urban systems, with smart healthcare emerging as a key sector. By leveraging sensors, Internet of Things (IoT) devices, and data analytics, smart healthcare aims to enhance service delivery and quality of life, particularly in response to urbanization challenges such as population growth [1]-[4]. Users are central to this ecosystem, both as data contributors and service beneficiaries. However, the diverse and sensitive nature of the data collected, particulary personal health data—necessitates robust privacy protection. Healthcare has become a primary target for data breaches, leading to heightened privacy concerns and user avoidance behaviors that hinder adoption and effectiveness [5]-[11]. This study focuses on users' perceptions of privacy protection in smart healthcare, particularly in terms of technical (e.g., encryption) and organizational (e.g., privacy policies) measures. Given their role as data owners, patients' engagement is vital to the success of smart healthcare services [12][13]. However, despite the availability of privacy-preserving technologies like blockchain, homomorphic encryption, and secure multi-party computation, users often lack awareness or confidence in these tools. The effectiveness of such measures is influenced not only by their technical strength but also by users' psychological perceptions of security [10][13][14][15].

User perceptions—shaped by factors such as perceived control, information risk, and expected societal benefits—significantly influence their willingness to disclose data and use smart healthcare services [16][17][18]. Technology acceptance models like UTAUT have been used to explore these dynamics, showing that while users recognize the benefits of digital health services, privacy and trust issues remain critical barriers to adoption [19][20]. These concerns are not just technical but deeply human, highlighting the need to bridge the gap between system design and user expectations. Despite growing attention, many studies still overlook the user's perspective on privacy protection. Limited awareness, passive consent, and a lack of empowerment persist due to the unequal power dynamics between users and service providers [13][21][22]. Effective communication of data protection measures is lacking, preventing users from making informed privacy decisions [23][24]. To advance smart healthcare adoption, future systems must prioritize transparency, user education, and privacy frameworks that align with user preferences and perceptions. This study aims to contribute by deepening the understanding of these user-centered concerns and informing more inclusive privacy strategies. To help users better protect and control their privacy, it is essential to improve the communication of privacy protection measures to users and raise their privacy awareness. The first step in this process is ensuring they perceive the privacy measures in place. Thus, it is crucial to address the research problem underlying this paper, namely, to understand users' perceptions of privacy protection measures in smart healthcare services. The paper is organized as follows. Section II outlines related work, theoretical foundations, and the research methodology. Section III presents the results, Section IV discusses their implications, and Section V concludes with key insights and future directions.

R.Q: How do users perceive privacy protection measures in smart healthcare services? The study aims to explore users' concerns and expectations when perceiving privacy protection measures in smart healthcare services. Understanding users' nuanced feelings is essential for designing privacy safeguards that are user-oriented, ensuring better alignment with users' privacy needs.

II. Research Baseline

Smart healthcare has emerged as a response to the increasing strain on traditional healthcare systems caused by population growth and rising disease prevalence. Leveraging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and mobile cloud computing, smart healthcare enhances communication, facilitates remote monitoring, and supports personalized treatment, diagnosis, and prevention efforts [25][26]. These services are broadly categorized into domains like location tracking, telehealth, mobile health, AI-driven diagnostics, and robotic systems [27]. Among these, five key application types are emphasized: tracking tools (e.g., Apple Watch), telehealth platforms (e.g., BetterHelp), AI-powered diagnostic systems (e.g., IBM Watson Health), integrated health information systems (e.g., Epic Systems), and medicine delivery platforms (e.g., Amazon Pharmacy). This study focuses on four types of smart healthcare services—wearable devices, mobile health management apps, telehealth platforms, and medicine delivery systems—due to their widespread user adoption and diverse data handling. These services directly involve users in managing vital signs, lifestyle data, medical records, and prescriptions. For example, wearable devices like Apple Health gather physiological data, while telehealth platforms support virtual consultations. These applications offer close user interaction, in contrast to more provider-centric systems such as Electronic Health Record (EHRs) or AI-assisted surgery, which are excluded from the study's scope. The selected services provide a relevant and practical basis for examining users' perceptions of privacy protection in smart healthcare.

Privacy Protection Measures: Smart healthcare systems face ongoing challenges in safeguarding user privacy throughout the data lifecycle, despite the many benefits they offer [11] [28]. To address these concerns, researchers have proposed various privacy protection strategies, including both technical and organizational measures. Organizational approaches such as privacy-by-policy, privacy-by-architecture, and privacy-by-design aim to embed privacy into system design, policy compliance, and user interactions from the outset [30]–[32]. These are further supported by regulatory frameworks like the GDPR and HIPAA, which enforce strict legal standards for personal health data handling. Organizational mechanisms such as consent management, transparency, and auditing play a key role in maintaining accountability and building trust [3]. Technically, privacy is protected through cryptographic methods, anonymization, data masking, access control, and advanced techniques like federated learning, homomorphic encryption, and secure multi-party computation [33]. Blockchain is also recognized for its privacy-enhancing attributes, including decentralization and transparency [6]. However, these measures often fall short in practice due to limited user control and inconsistent implementations across centralized and decentralized environments [23]. Many existing solutions remain too provider-centric, failing to fully address user needs or empower them in managing their own data [6, 11]. As such, there is a pressing need for privacy strategies that incorporate users' perspectives more effectively and bridge the gap between technical safeguards and user-centric privacy experiences.

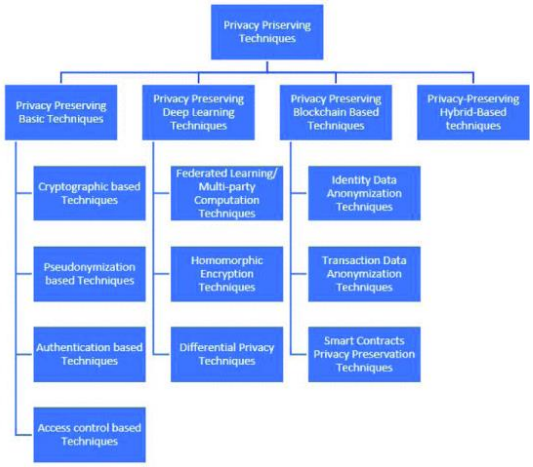

Figure 1. Privacy-preserving Techniques Taxonomy [33]

Theories and Factors Shaping Users' Perception and Adoption: Users' perceptions significantly influence their intention to adopt smart healthcare services, as outlined in established frameworks like the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) [35][36]. TAM focuses on perceived usefulness and ease of use, while UTAUT highlights performance expectancy, effort expectancy, social influence, and facilitating conditions. These models are further enriched by the privacy calculus theory, which balances perceived benefits against privacy risks [37][38]. Research shows that risks such as data misuse, legal vulnerabilities, and lack of control affect users' protective behaviors, while perceived benefits like better healthcare and contributions to research often encourage data sharing [9, 39]. Emotions, cognitive biases, and contextual factors also shape decision-making. Although privacy remains a concern, users often prioritize perceived benefits, especially when immediate rewards or limited privacy knowledge come into play [40]–[42]. Older adults, for instance, tend to accept privacy risks over time, leading to a resigned attitude toward potential misuse [43]. For wearables, adoption hinges on a risk-benefit evaluation tied to data sensitivity and regulatory protections [44]. However, challenges like opaque privacy notices and cognitive overload hinder informed decisions [45–47]. Emerging factors—such as trust in AI, personalization, and digital literacy—further affect adoption, prompting scholars to recommend tailoring acceptance models to specific healthcare contexts [48]–[51]. This study adopts relevant theoretical constructs to capture the nuanced dimensions of user perception in smart healthcare.

A. Method Application

This study employs a qualitative, interview-based survey strategy to explore users' perceptions of privacy protection in

smart healthcare services. Qualitative surveys effectively reveal nuanced behaviors, perceptions, and attitudes, making them particularly suitable for understanding complex interactions between privacy risks, benefits, and other factors [52][53]. To ensure rigor and reliability, this study integrates standardized theoretical frameworks, including the taxonomy of privacy-preserving techniques [33], Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), and privacy calculus theory, to guide interview design and analysis [54]. These frameworks help structure the interview questions effectively by addressing key constructs such as perceived ease of use, social influence, performance expectancy, perceived usefulness, perceived privacy risks, and perceived benefits. Interviews are conducted individually through audio calls on WhatsApp and WeChat, recorded and transcribed using the iOS Voice Memos application for English and Tongyi.ai for Chinese interviews. Recordings are solely for transcription accuracy and verification purposes, ensuring data reliability. **Sampling:**This study employs non-probability purposive sampling, deliberately selecting participants aged 18–65 from urban areas in Europe, North America, and Asia who possess prior experience with smart healthcare services and basic privacy protection knowledge, ensuring their relevance to the research topic [56]. Probability sampling was not chosen due to the need for informed participants rather than random selection. Ethical considerations and resource constraints excluded minors, individuals over 65, and rural populations, as these groups pose consent challenges or may lack familiarity with smart healthcare [13]. The target sample size is approximately 10 participants, consistent with qualitative research standards indicating saturation typically occurs between 10 to 12 interviews [61] [62]. Interviews lasting 60–90 minutes ensure comprehensive coverage of key points, enhancing study validity despite the limited sample size. Convenience sampling was dismissed due to its potential limitations in participant diversity and relevance [56]. **Data Analysis:** The study analyzes interview data using Thematic Analysis (TA), a widely adopted qualitative method suitable for identifying patterns and themes within interview transcripts [63][64]. Following the six-step process outlined by Braun and Clarke [65], the analysis begins by coding relevant keywords, refining codes to eliminate redundancy, and categorizing them into themes. This study adopts a hybrid thematic approach, primarily utilizing inductive thematic analysis to allow patterns to emerge naturally, complemented by deductive analysis based on constructs from the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), and privacy calculus theory to enhance objectivity and validity [66]-[69]. NVivo software is employed to improve analytical efficiency, data management, and accuracy [70, 71]. Content analysis was considered but not selected due to its limited ability to capture contextual and latent meanings critical to the research [56] [72] [73].

III. Result

This study applied thematic analysis supported by NVivo software, following the structured six-step process outlined by [65]. Initial coding involved careful review of interview transcripts, capturing significant insights and relating these to theoretical frameworks. Notably, participant uncertainties, such as limited knowledge about privacy protection, were documented. The code "Cumbersome Authentication Process" drew upon "perceived ease of use" from the TAM and "effort expectancy" from the Unified Theory of Acceptance and Use of Technology (UTAUT). In total, 21 initial codes emerged. From these codes, themes and subthemes were developed, categorizing user perceptions into positive and negative dimensions. A prominent theme identified was the "Disadvantaged Position of Users in Protecting Their Privacy," with the subtheme "Insufficient Right to be Informed," consistently emphasized by participants. Conversely, positive perceptions were encapsulated under the theme related to "facilitating conditions" from UTAUT, distinguishing between external support (Oversight and Constraints) and internal support (Internal Handling). Redundant codes were subsequently refined, reducing them to 12 cohesive codes. For instance, "Unknown Technical Principles" merged into "Unknown Implementation Process," reflecting users' practical concerns rather than theoretical knowledge. Similarly, "Insufficient Engagement" was incorporated into "Lack of User Data Management," categorized under the subtheme "Insufficient Control." Ultimately, the refined analysis identified three main themes and seven subthemes from the dataset.

A. The Disadvantaged Position of Users in Protecting Their Privacy:

Users' Perceived Vulnerability in Privacy Protection Thematic analysis revealed users feel disadvantaged in safeguarding their privacy within smart healthcare services, reflecting concerns from privacy calculus theory. Despite existing measures, users often lack perceived control and awareness, particularly in three key areas: unknown personnel, unclear implementation processes, and uncertain effectiveness of results. Users expressed concerns about not knowing who accesses their data, especially with vague or opaque privacy policies and multi-party access scenarios. Many feared unauthorized third-party data sharing, particularly for commercial purposes, while showing more openness toward research uses, provided transparency and consent are maintained.

Lack of Transparency Undermines Trust: Participants emphasized that unfamiliar technical implementations (e.g., encryption, anonymization) raise doubts, especially when not clearly explained. Even tech-savvy users sought clarity on compatibility and deployment, while others feared such terms masked hidden costs or misuse. Vague legal language in privacy policies also contributed to uncertainty about data handling. Users wanted clear, example-driven explanations of practices and desired features like access logs, deletion confirmation, and visual cues for encryption. Ultimately, the study highlights how insufficient transparency undermines

TABLE I. THEMES, SUBTHEMES, AND CORRESPONDING CODES

Themes	Subthemes	Codes
The Disadvantaged Position of Users in Protecting Their Privacy	Insufficient Right to be Informed	Unknown Personnel Involved
		Unknown Implementation Process
		Unknown Effectiveness of Results
	Insufficient Control	Lack of User Data Management
		Passive Choice in Privacy Policy
Privacy Reassurance	Oversight and Constraints	Legal Regulations and Audits
	Technical Reliability	Multi-Layer Protection
	Internal Handling	Updates of Privacy Policy
		Thoughtful Data Breach Response
User Experience Barriers	Operational Barriers	Cumbersome Authentication Process
		Unclear Position of the Privacy Policy
	Cognitive Barriers	Long and Obscure Privacy Policy

users' sense of security, making trust in privacy protections contingent on clarity, informed consent, and demonstrable effectiveness. **Users' Limited Control and Data Deletion Challenges:** Participants expressed a strong sense of limited control over their data within smart healthcare services, often feeling reliant on providers who possess technical knowledge and control system configurations. This asymmetry reinforces user vulnerability, as providers determine how and when data is used [45]. While participants desired more autonomy—such as opt-in/out capabilities for data use, the ability to delete records post-service, and clearer management of access rights—these features remain inadequately supported. Even in GDPR-covered regions, deletion processes are often slow, indirect, or poorly designed, further disempowering users. Participants from outside the GDPR context reported even fewer deletion options, highlighting global inconsistencies in privacy control.

Inadequate Consent and Forced Privacy Agreements: Granular consent management was viewed as essential, with users preferring settings that allow them to specify the purpose, scope, and recipients of shared data. However, participants described being forced into "take it or leave it" agreements during account registration, where refusing a privacy policy meant losing access to the service entirely [46]. This coercive design fosters mistrust in both the policies and the providers themselves, though it doesn't always deter usage, especially when the service is deemed necessary. Participants emphasized that privacy policies often serve as compliance tools rather than genuine efforts to respect user preferences [5][46]. To restore meaningful control, users should be empowered to use core services even if they partially or fully reject privacy terms.

B. Privacy Reassurance:

Legal Compliance as a Source of Reassurance: Participants expressed generally positive views toward privacy regulations like the GDPR and HIPAA, associating compliance with increased confidence in smart healthcare services. GDPR compliance, in particular, was seen as a strong indicator of trustworthy data practices due to its well-defined principles, independent oversight, and strict penalties for violations . Some participants emphasized that GDPR offers not only legal assurance but also actionable tools for users to verify compliance and seek redress. In contrast, while HIPAA was acknowledged for setting essential standards, American participants showed relatively lower confidence in its enforcement and practical application. This suggests that users value legal frameworks more when they are backed by demonstrable enforcement mechanisms and transparent rights protections.

The Role of Audits in Reinforcing Trust: External audits were highlighted as a crucial organizational safeguard complementing legal compliance. Participants emphasized that while privacy-enhancing technologies like encryption and anonymization are important, their trust increases when these measures are validated through transparent third-party audits. Audits conducted by reputable firms enhance users' perception of provider accountability, particularly because users often lack the expertise to evaluate technical safeguards themselves. Together, legal constraints and professional audits offer layered protection that aligns with the UTAUT framework's notions of performance expectancy and facilitating conditions, reinforcing users' belief that their privacy is both respected and technically safeguarded.

Multi-layer Protection and Technical Confidence Participants expressed strong support for multi-layer privacy protection, noting that the combination of various techniques—such as encryption, anonymization, and multi-factor authentication—enhanced their trust in smart healthcare systems. While many users lacked technical expertise, they believed that layering different methods could reduce single points of failure and increase reliability. Features like two-factor authentication were especially appreciated, as they offered visible, user-facing indicators of security. This sense of reassurance directly influenced users' willingness to engage with smart healthcare services, aligning with the UTAUT construct of performance expectancy. **Proactive Provider Measures and Breach Response** Users also valued internal organizational practices, such as timely updates to privacy policies and responsive actions following data breaches, as signs of a provider's commitment to privacy protection. Regular policy updates, when clearly communicated, reassured participants that providers were keeping pace with technological and legal changes. After a breach, participants expected prompt notifications, transparency about affected data, and evidence of corrective action—such as improved security systems or audits. These proactive and reflective efforts serve as key facilitating conditions that influence continued user trust, even after a privacy incident. Providers who effectively communicate updates and breach responses are more likely to retain user confidence in the long term.

Cognitive Barriers to Understanding Privacy Policies: Participants widely reported cognitive challenges when engaging with privacy policies, citing long, text-heavy documents and complex legal jargon as key deterrents to reading or understanding them. These barriers were especially burdensome for older users, who also faced physical and digital literacy limitations. The confusing presentation and obscure terminology led to user frustration and mistrust, with some perceiving the complexity as an intentional obfuscation by providers. Participants suggested clearer formats like visual checklists, interactive summaries, and plain language versions to improve comprehension and enhance trust. Offering two parallel policy versions—one simplified and one legally detailed—was proposed to balance accessibility with compliance requirements.

Operational Barriers and Their Contextual Impact: Operational hurdles, particularly around authentication processes, were another major concern. Users found complex password requirements and recovery procedures burdensome, especially when compounded by poor connectivity or urgent health needs. While users accepted stricter authentication for high-risk services like mental health or prescriptions, they preferred minimal friction for lower-risk tasks like symptom checking or step tracking. Participants also noted difficulty locating privacy policies within app interfaces, which undermined their perceived importance. Although this didn't always affect service use directly, it shaped negative impressions of provider transparency. Users emphasized the need for adaptive privacy measures and intuitive design that aligns security requirements with task sensitivity and user context.

IV. Discussion

This study reveals that users generally view privacy protection measures in smart healthcare positively, particularly when multi-layer safeguards—such as encryption, anonymization, and multi-factor authentication—are employed, reinforcing their sense of security and aligning with UTAUT's performance expectancy construct. However, users also expressed concerns about limited transparency and control, especially when faced with complex or opaque privacy policies. Legal frameworks like the GDPR and HIPAA, along with third-party audits, were seen as crucial external supports that help balance the power disparity between users and providers [29][38]. Despite recognizing these safeguards, users often felt disempowered due to their lack of technical or legal literacy, particularly in urgent health situations where privacy is traded for immediate care needs [9][21][42]. These tensions echo the privacy calculus theory, where perceived privacy risks reduce trust and adoption willingness [44], though this is sometimes overridden by brand trust or social influence [19]. Users' perceptions of privacy risk vary based on the type of smart healthcare service and the sensitivity of data involved. Telehealth platforms were seen as higher risk due to their handling of sensitive medical histories, while wearable devices and mobile health apps were perceived as lower risk depending on context [9][40][41]. Unique concerns were also raised about medicine delivery services, particularly involving the disclosure of home addresses in offline interactions. These findings emphasize that privacy protections must be contextually adaptive. The study contributes to the literature by highlighting the often-overlooked user perspective, suggesting refinements to existing models like UTAUT and the privacy calculus theory, and offering actionable recommendations to enhance transparency, control, and user empowerment in smart healthcare design.

V. CONCLUSIONS AND FUTURE WORK

This study investigates users' perceptions of privacy protection measures in smart healthcare through interviews with diverse participants, uncovering both negative and positive views. Negative perceptions largely stem from users' lack of transparency and control—such as not knowing who accesses their data, limited ability to manage or delete it, and being

compelled to accept unclear privacy policies. Participants also faced cognitive and operational challenges, including overly complex policies and cumbersome authentication. In contrast, users responded positively to multi-layer technical safeguards, legal and audit oversight, and providers' proactive actions like transparent updates and breach responses. These findings emphasize the need for privacy strategies that are more user-centric, accessible, and empowering. Despite using established theoretical frameworks and rigorous qualitative methods, the study's small, purposive sample limits the generalizability of findings, particularly to minors and older populations. It also lacks analysis of how demographic factors or specific service contexts influence perceptions. Future research should incorporate mixed-method approaches to enable cross-cultural and service-specific comparisons. Additionally, a deeper theoretical integration of models such as TAM, UTAUT, and privacy calculus theory is recommended to refine concepts such as perceived transparency and risk. Practically, future work should develop tailored privacy design guidelines aligned with real-world healthcare applications, such as embedding user-focused encryption in telehealth platforms.

REFERENCES

[1] V. Garcia-Font, "SocialBlock: An architecture for decentralized user-centric data management applications for communications in smart cities," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 13–23, Nov. 2020. doi: 10.1016/j.jpdc.2020.06.004

[2] V. Zimmermann, "Smart cities as a testbed for experimenting with humans? - Applying psychological ethical guidelines to smart city interventions," *Ethics and Information Technology*, vol. 25, no. 4, p. 54, Oct. 2023. doi: 10.1007/s10676-023-09729-3

[3] D. Eckhoff and I. Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 489–516, 2018. doi: 10.1109/COMST.2017.2748998

[4] J. Sanghavi, "Review of Smart Healthcare Systems and Applications for Smart Cities," in *ICCCE 2019*, A. Kumar and S. Mozar, Eds. Singapore: Springer Singapore, 2020, pp. 325–331.

[5] European Union, "General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[6] D. El Majdoubi, H. El Bakkali, S. Sadki, Z. Maqour, and A. Leghmid, "The Systematic Literature Review of Privacy-Preserving Solutions in Smart Healthcare Environment," *Security and Communication Networks*, vol. 2022, no. 1, p. 5642026, 2022. doi: 10.1155/2022/5642026

[7] Y. Li, "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems*, vol. 28, pp. 453–496, Jan. 2011. doi: 10.17705/1CAIS.02828

[8] S. R. Simon, J. S. Evans, A. Benjamin, D. Delano, and D. W. Bates, "Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study," *Journal of Medical Internet Research*, vol. 11, no. 3, p. e30, 2009. doi: 10.2196/jmir.1164

[9] X. Deng, D. Wang, and L. Yang, "The Impact of Perceived Risk on Online Medical Users' Privacy Protection Behavior," in *Proc. 27th Int. Conf. on Computer Supported Cooperative Work in Design (CSCWD)*, May 2024, pp. 1238–1243. doi: 10.1109/CSCWD61410.2024.10580280

[10] A. Odeh, A. Eman, and S. Walid, "Privacy-Preserving Data Sharing in Telehealth Services," *Applied Sciences*, 2024. doi: 10.3390/app142310808

[11] M. A. Sahi *et al.*, "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," *IEEE Access*, vol. 6, pp. 464–478, 2018. doi: 10.1109/ACCESS.2017.2767561

[12] D. E. Majdoubi, H. E. Bakkali, S. Sadki, A. Leghmid, and Z. Maqour, "HOPPy: Holistic Ontology for Privacy-Preserving in Smart Healthcare environment," in *Proc. 2021 Fifth World Conf. on Smart Trends in Systems Security and Sustainability (WorldS4)*, 29–30 July 2021, pp. 248–253. doi: 10.1109/WorldS451998.2021.9514051

[13] F. Tazi, A. Nandakumar, J. Dykstra, P. Rajivan, and S. Das, "SoK: Analyzing Privacy and Security of Healthcare Data from the User Perspective," *ACM Trans. Comput. Healthcare*, vol. 5, no. 2, p. Article 11, 2024. doi: 10.1145/3650116

[14] C.-L. Hsu and M.-R. Lee, "User acceptance of a community-based healthcare information system preserving user privacy," in *Universal Access in Human-Computer Interaction. Applications and Services for Quality of Life: Proc. 7th Int. Conf. UAHCI 2013, Part III*, Las Vegas, USA, July 21–26, 2013. Springer, pp. 453–462.

[15] S. M. E. Sepasgozar, S. Hawken, S. Sargolzaei, and M. Foroozanfa, "Implementing citizen centric technology in developing smart cities: A model for predicting the acceptance of urban technologies," *Technological Forecasting and Social Change*, vol. 142, pp. 105–116, 2019. doi: 10.1016/j.techfore.2018.09.012

[16] E. M. Schomakers, C. Lidynia, and M. Ziefle, "Listen to My Heart? How Privacy Concerns Shape Users' Acceptance of e-Health Technologies," in *2019 Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 21–23 Oct. 2019, pp. 306–311. doi: 10.1109/WiMOB.2019.8923448

[17] A. Kharlamov, R. Hohmann, and G. Parry, "Data sharing decisions: Perceptions and intentions in healthcare," *Strategic Change*, vol. 32, no. 6, pp. 223–237, 2023.

[18] E. Princi and N. C. Krämer, "Out of control – privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices," *Frontiers in Psychology*, vol. 11, p. 582054, 2020.

[19] Y.-J. Moon and Y.-H. Hwang, "A Study of Effects of UTAUT-Based Factors on Acceptance of Smart Health Care Services," in *Advanced Multimedia and Ubiquitous Engineering*, J. J. Park, H.-C. Chao, H. Arabnia, and N. Y. Yen, Eds. Berlin, Heidelberg: Springer, 2016, pp. 317–324.

[20] E. Pouyan, "The Impacts of the Perceived Transparency of Privacy Policies and Trust in Providers for Building Trust in Health Information Exchange: Empirical Study," *JMIR Medical Informatics*, vol. 7, 2019. doi: 10.2196/preprints.14050

[21] K. Halvorsen *et al.*, "Empowerment in healthcare: A thematic synthesis and critical discussion of concept analyses of empowerment," *Patient Education and Counseling*, vol. 103, no. 7, pp. 1263–1271, Jul. 2020. doi: 10.1016/j.pec.2020.02.017

[22] M. Duckert and L. Barkhuus, "Protecting Personal Health Data through Privacy Awareness: A study of perceived data privacy among people with chronic or long-term illness," *Proc. ACM Hum.-Comput. Interact.*, vol. 6, no. GROUP, p. Article 11, 2022. doi: 10.1145/3492830

[23] M. N. Alraja, H. Barhamgi, A. Rattrout, and M. Barhamgi, "An integrated framework for privacy protection in IoT — Applied to smart healthcare," *Computers & Electrical Engineering*, vol. 91, p. 107060, May 2021. doi: 10.1016/j.compeleceng.2021.107060

[24] S. M. Williamson and V. Prybutok, "Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare," *Applied Sciences*, vol. 14, no. 2, p. 675, 2024. [Online]. Available: https://www.mdpi.com/2076-3417/14/2/675

[25] S. S. Raoof and M. A. S. Durai, "A Comprehensive Review on Smart Health Care: Applications, Paradigms, and Challenges with Case Studies," *Contrast Media & Molecular Imaging*, vol. 2022, no. 1, p. 4822235, 2022. doi: 10.1155/2022/4822235

[26] M. A. Jabbar, K. M. V. V. Prasad, and R. Aluvalu, "Reimagining the Indian Healthcare Ecosystem with AI for a Healthy Smart City," in *Emerging Technologies in Data Mining and Information Security*, A. E. Hassanien, S. Bhattacharyya, S. Chakrabati, A. Bhattacharya, and S. Dutta, Eds. Singapore: Springer, 2021, pp. 543–551.

[27] H. Kwon *et al.*, "Review of smart hospital services in real healthcare environments," *Healthcare Informatics Research*, vol. 28, no. 1, pp. 3–15, 2022.

[28] A. Algarni, "A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems," *IEEE Access*, vol. 7, pp. 101879–101894, 2019. doi: 10.1109/ACCESS.2019.2930962

[29] H. Liu, X. Yao, T. Yang, and H. Ning, "Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-Based Smart Health," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1352–1362, 2019. doi: 10.1109/JIOT.2018.2843561

[30] S. Spiekermann and L. F. Cranor, "Engineering Privacy," *IEEE Transactions on Software Engineering*, vol. 35, no. 1, pp. 67–82, 2009. doi: 10.1109/tse.2008.88

[31] A. A. Alghanim, S. M. M. Rahman, and M. A. Hossain, "Privacy Analysis of Smart City Healthcare Services," in *Proc. 2017 IEEE Int. Symp. on*

Multimedia (ISM), 11–13 Dec. 2017, pp. 394–398. doi: 10.1109/ISM.2017.79

[32] C. Montes *et al.*, "A flexible, privacy enhanced and secured ICT architecture for a smart grid project with active consumers in the city of Zwolle—NL," in *22nd Int. Conf. and Exhibition on Electricity Distribution (CIRED 2013)*, IET, 2013, pp. 1–4.

[33] B. R. Louassef and N. Chikouche, "Privacy preservation in healthcare systems," in *Proc. 2021 Int. Conf. on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*, 20–21 Nov. 2021, pp. 1–6. doi: 10.1109/AI-CSP52968.2021.9671083

[34] A. Dangi and R. Mogili, "Privacy Preservation Measure using t-closeness with combined l-diversity and k-anonymity," *Int. J. of Advanced Research in Computer Science and Electronics Engineering*, vol. 1, pp. 28–33, 2012.

[35] A. A. AlQudah, M. Al-Emran, and K. Shaalan, "Technology Acceptance in Healthcare: A Systematic Review," *Applied Sciences*, vol. 11, no. 22, p. 10537, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/22/10537

[36] S. Attuquayefio and H. Addo, "Review of studies with UTAUT as conceptual framework," *European Scientific Journal*, vol. 10, no. 8, 2014.

[37] E.-M. Schomakers, C. Lidynia, and M. Ziefle, "The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance," *Int. J. of Human–Computer Interaction*, vol. 38, no. 13, pp. 1276–1289, 2022. doi: 10.1080/10447318.2021.1994211

[38] S. Li *et al.*, "Research on user's highly sensitive privacy disclosure intention in home intelligent health service system: A perspective from trust enhancement mechanism," *DIGITAL HEALTH*, vol. 9, p. 20552076231219444, 2023. doi: 10.1177/20552076231219444

[39] D. Grande, N. Mitra, A. Shah, F. Wan, and D. A. Asch, "Public preferences about secondary uses of electronic health information," *JAMA Intern Med*, vol. 173, no. 19, pp. 1798–1806, Oct. 2013. doi: 10.1001/jamainternmed.2013.9166

[40] M. S. Rahman, "Does Privacy Matter When We are Sick? An Extended Privacy Calculus Model for Healthcare Technology Adoption Behavior," in *Proc. 2019 10th Int. Conf. on Information and Communication Systems (ICICS)*, 11–13 June 2019, pp. 41–46. doi: 10.1109/IACS.2019.8809175

[41] D. Kim, K. Park, Y. Park, and J.-H. Ahn, "Willingness to provide personal information: Perspective of privacy calculus in IoT services," *Computers in Human Behavior*, vol. 92, pp. 273–281, Mar. 2019. doi: https://doi.org/10.1016/j.chb.2018.11.022

[42] G. Fox, ""To protect my health or to protect my health privacy?" A mixed-methods investigation of the privacy paradox," *Journal of the Association for Information Science and Technology*, vol. 71, no. 9, pp. 1015–1029, 2020.

[43] T. Schroeder, M. Haug, and H. Gewald, "Data Privacy Concerns Using mHealth Apps and Smart Speakers: Comparative Interview Study Among Mature Adults," *JMIR Formative Research*, vol. 6, no. 6, 2022. doi: 10.2196/28025

[44] H. Li, J. Wu, Y. Gao, and Y. Shi, "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective," *Int. J. of Medical Informatics*, vol. 88, pp. 8–17, Apr. 2016. doi: https://doi.org/10.1016/j.ijmedinf.2015.12.010

[45] A. Acquisti *et al.*, "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Comput. Surv.*, vol. 50, no. 3, p. Article 44, 2017. doi: 10.1145/3054926

[46] F. Schaub, R. Balebako, and L. F. Cranor, "Designing Effective Privacy Notices and Controls," *IEEE Internet Computing*, vol. 21, no. 3, pp. 70–77, 2017. doi: 10.1109/MIC.2017.75

[47] M. W. Vail, J. B. Earp, and A. I. Antón, "An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies," *IEEE Trans. on Engineering Management*, vol. 55, pp. 442–454, 2008.

[48] K. Liu and D. Tao, "The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services," *Computers in Human Behavior*, vol. 127, p. 107026, Feb. 2022. doi: https://doi.org/10.1016/j.chb.2021.107026

[49] B. Watjatrakul, "Intention to use a free voluntary service: The effects of social influence, knowledge and perceptions," *Journal of Systems and Information Technology*, vol. 15, 2013. doi: 10.1108/13287261311328903

[50] R. Holden and B.-T. Karsh, "The Technology Acceptance Model: Its Past and Its Future in Health Care," *Journal of Biomedical Informatics*, vol. 43, pp. 159–172, Aug. 2009. doi: 10.1016/j.jbi.2009.07.002

[51] V. Braun, V. Clarke, E. Boulton, L. Davey, and C. McEvoy, "The online survey as a qualitative research tool," *International Journal of Social Research Methodology*, vol. 24, pp. 641–654, 2020.

[52] Z. N. Ghafar, "Evaluation Research: A Comparative Analysis of Qualitative and Quantitative Research Methods," *Middle East Research Journal of Linguistics and Literature*, 2023.

[53] J. Melegati, K. Conboy, and D. Graziotin, "Qualitative Surveys in Software Engineering Research: Definition, Critical Review, and Guidelines," *IEEE Transactions on Software Engineering*, vol. 50, pp. 3172–3187, 2024.

[54] K. Semyonov-Tal, "Keeping medical information safe and confidential: a qualitative study on perceptions of Israeli physicians," *Israel Journal of Health Policy Research*, vol. 13, no. 1, p. 54, Sep. 2024. doi: 10.1186/s13584-024-00641-9

[55] M. Denscombe, *The Good Research Guide for Small-Scale Social Research Projects*, 7th ed. Maidenhead, England: Open University Press, 2021.

[56] S. Y. Chyung, M. Kennedy, and I. A. Campbell, "Evidence-Based Survey Design: The Use of Ascending or Descending Order of Likert-Type Response Options," *Performance Improvement*, vol. 57, pp. 9–16, 2018.

[57] S. Rahman, "The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review," *Journal of Education and Learning*, vol. 6, pp. 102–112, 2016.

[58] A. E. Mueller and D. L. Segal, "Structured versus semistructured versus unstructured interviews," *The Encyclopedia of Clinical Psychology*, vol. 1, no. 7, 2014.

[59] United Nations Statistical Office, "Provisional guidelines on standard international age classifications," in *Statistical Papers*, New York: United Nations, 1982.

[60] Y. Lu, M. Jian, N. Muhamad, and M. Hizam-Hanafiah, "Data saturation in qualitative research: A literature review in entrepreneurship study from 2004–2024," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 12, p. 9753, 2024.

[61] D. M. Turner-Bowker *et al.*, "Informing a priori sample size estimation in qualitative concept elicitation interview studies for clinical outcome assessment instrument development," *Value in Health*, vol. 21, no. 7, pp. 839–842, 2018.

[62] C. Herzog, C. Handke, and E. Hitters, "Analyzing Talk and Text II: Thematic Analysis," in *The Palgrave Handbook of Methods for Media Policy Research*, H. Van den Bulck, M. Puppis, K. Donders, and L. Van Audenhove, Eds. Cham: Springer International Publishing, 2019, pp. 385–401.

[63] C. Herzog, C. Handke, and E. Hitters, "Analyzing Talk and Text II: Thematic Analysis," 2019. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068081

[64] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, pp. 77–101, 2006. doi: 10.1191/1478088706qp063oa

[65] S. Elo and H. Kyngäs, "The qualitative content analysis process," *Journal of Advanced Nursing*, vol. 62, no. 1, pp. 107–115, 2008. doi: 10.1111/j.1365-2648.2007.04569.x

[66] J. Fereday and E. Muir-Cochrane, "Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development," *International Journal of Qualitative Methods*, vol. 5, no. 1, pp. 80–92, 2006. doi: 10.1177/160940690600500107

[67] C. H. Saunders *et al.*, "Practical thematic analysis: a guide for multidisciplinary health services research teams engaging in qualitative analysis," *BMJ*, vol. 381, 2023.

[68] K. A. Campbell *et al.*, "Reflexive thematic analysis for applied qualitative health research," *The Qualitative Report*, vol. 26, no. 6, pp. 2011–2028, 2021.

[69] L. Wong, "Data analysis in qualitative research: a brief guide to using NVivo," *Malaysian Family Physician*, vol. 3, no. 1, pp. 14–20, 2008.

[70] M. I. Azeem and N. A. Salfi, "Usage of NVivo software for qualitative data analysis," 2012.

[71] I. Elgammal, "Content Analysis," in *Encyclopedia of Tourism*, J. Jafari and H. Xiao, Eds. Cham: Springer Nature Switzerland, 2024, pp. 207–208.

[72] R. K. Reger and P. A. Kincaid, "Content and Text Analysis Methods for Organizational Research," Oxford University Press, 2021.

[73] R. Dubinsky, "PNS169 Personal Medical Health Records Regulation in the United States, European Union and Israel," *Value in Health*, vol. 22, pp. S789–S790, 2019.

[74] C. J. Hoofnagle and J. King, "What Californians Understand About Privacy Online," *Available at SSRN 1133075*, 2008. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075