Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4288-cd

A Position on Rethinking HCI Practices in Dynamic Consent: Balancing Privacy, Trust, Safety, and Risk Communication for Enhanced System Reliability

Sabarathinam Chockalingam

Department of Risk and Security, Institute for Energy Technology, Norway. E-mail: Sabarathinam.Chockalingam@ife.no

Petter Kvalvik

Department of Business Development, Institute for Energy Technology, Norway. E-mail: Petter.Kvalvik@ife.no

Sizarta Sarshar

Department of Risk and Safety, Institute for Energy Technology, Norway. E-mail: Sizarta.Sarshar@ife.no

As systems in Human-Computer Interaction (HCI) and the Internet of Things (IoT) evolve, traditional consent models are increasingly inadequate to address the challenges of privacy, trust, safety, and risk management. Static, one-time consent mechanisms fail to keep pace with the dynamic nature of data-driven interactions and autonomous devices. This paper explores the potential of dynamic consent as a conceptual framework for enhancing user control, system reliability, and risk management in HCI. Dynamic consent provides a flexible, adaptive approach to consent that allows users to adjust their preferences in real-time, promoting transparency, privacy, and trust while reducing consent fatigue. This is crucial in IoT contexts where systems operate autonomously, collecting data passively with minimal user interaction. Furthermore, the cross-border flow of data presents complexities in consent management, as consent across digital borders must respect different jurisdictional regulations while protecting individual rights. This paper explores the interplay between dynamic consent and key concepts such as digital sovereignty, where individuals maintain control over their digital identity, and consent fatigue, which erodes user engagement, and trust. As data becomes a valuable commodity within data markets and digital value chains, data reuse requires flexible consent models that ensure transparency. It argues that while static consent models undermine privacy and trust, dynamic consent offers a more flexible and adaptive approach. This approach allows users to adjust their consent preferences in real-time, reducing consent fatigue and improving system transparency. Instead of proposing specific solutions, this paper advocates for rethinking HCI practices within the context of dynamic consent, particularly in the area of risk communication. To that end, we address the following Research Question (RQ): How can dynamic consent be framed to balance privacy, trust, safety, and risk management in Human-Computer Interaction?

Keywords: Autonomy, Digital Sovereignty, HCI, IoT, Privacy, Risk, Safety, Transparency, Trust.

1. Introduction

The evolution of Internet of Things (IoT) has transformed how users interact with digital systems. As digital ecosystems increasingly depend on user consent for data collection and sharing, dynamic consent has emerged as a flexible and user-centric approach that allows individuals to modify or withdraw their consent over time (Kaye et al. 2015). Unlike static consent, which is typically a one-time agreement, dynamic consent provides continuous user control and transparency, ensuring compliance with evolving privacy regulations such as the General Data Protection Regulation (GDPR). Despite numerous efforts to implement dynamic consent across various domains, a comprehensive overview is still lacking. Existing studies tend to focus on specific aspects, such as technical implementations and sector-specific use cases, without analysing how dynamic consent addresses key principles like privacy, user control, transparency, and trust.

To that end, this study conducts a Systematic Literature Review (SLR) to examine the current landscape of dynamic consent. Furthermore, we analyze the identified studies using three comparison criteria: (i) application domains and target groups, (ii) key aspects addressed (privacy, user control, transparency, trust), and (iii) elements/sub-elements of the digital consent management process. Importantly, risk communication, defined as the ability to inform users about potential safety and security risks that affect privacy in an intuitive and accessible manner, remains underexplored, mainly in the context of user-facing transparency dashboards. Without effective HCI-driven solutions, users may struggle understanding their consent choices, leading to consent fatigue, decreased trust, and potential privacy risks.

The remainder of this paper is structured as follows: Section 2 provides background on static and dynamic consent, as well as the key functional elements of consent management. Section 3 reviews related work, while Section 4 outlines the SLR methodology. Section 5 presents findings on application domains, target groups, and key aspects of dynamic consent. Section 6 discusses the need for improved HCI in user-facing transparency dashboards and risk communication. Finally, Section 7 provides conclusions and future work directions.

2. Background

2.1. *Static and Dynamic Consent Management*

In static consent systems, consent is obtained at the time of data collection for all future uses of that data (Thapa et al. 2021). For instance, a patient might provide static consent when filling out a medical form, allowing their data to be used for treatment and research purposes. Once given, this consent typically remains unchanged unless the patient explicitly revises it. However, if the data is later used for new purposes, such as being shared with third-party researchers or used in a different type of medical study, the initial consent may not fully cover these new uses. This highlights a limitation of static consent as it does not allow for ongoing adjustments to the scope of data usage over time (Thapa et al. 2021). Furthermore, static consent systems often lack continuous user control, leaving users unaware of how their data is being used.

In contrast, dynamic consent management allows users to update or revoke their consent at any time during their interactions with a service (Kaye et al. 2015). For instance, in the context of IoT, a wearable device that continuously collects health data such as heart rate and sleep patterns, may periodically prompt the user to review their consent. This allows users to adjust how their data is shared, such as opting out of sharing sleep data with third-party applications or granting additional permissions for medical research. Users can also receive notifications about how their data is being used and modify their preferences as needed. Dynamic consent helps ensure compliance with evolving data protection laws such as the European Union (EU)'s GDPR, by keeping users informed and maintaining control over their data (Merlec et al. 2021). However, frequent updates and notifications may lead to information overload or confusion, especially if the user interface is poorly designed or the data presented in the HCI is unclear (Schuler Scott. 2022).

2.2. *Consent Management Process: Key Functional Elements*

This section outlines key functional elements of digital consent management. The main components include: (i) identification and authentication, (ii) core consent management, and (iii) portability management (Lähteenoja et al. 2024).

(i) Identification and Authentication ensure that users can be reliably identified and re-identified, enabling them to modify or withdraw consent as needed. This process can involve methods ranging from username and password combinations to more secure options, such as bank IDs, depending on legal and regulatory requirements.

(ii) Core Consent Management covers the entire process of handling consent, from initial collection to subsequent modifications and revocations. A key component is the "user-facing transparency dashboard", which

provides users a clear overview of all the consents they have granted. Through this dashboard, users can easily review, update, or withdraw consent at any time. It ensures transparency by providing detailed information about the data being collected, its sources, and how it will be used, along with privacy risk information. This enables users to make informed decisions and retain control over their personal data.

(iii) Portability Management focuses on enabling users to access or transfer their data after giving consent, allowing them more flexibility in managing their information. Personal data storage simplifies future consent interactions by storing commonly shared data, eliminating the need for users to re-enter the same information repeatedly.

3. Related Work

Several reviews and applications have focused on dynamic consent. (Lay et al. 2025) provided an overview of the 31 key benefits and 8 challenges associated with dynamic consent platforms. Their study emphasizes how dynamic consent empowers individuals to retain more control over their personal data and provide enhanced flexibility in data sharing over time. It also highlights challenges, including the digital divide and consent fatigue. (Lee et al. 2024) investigated the application of dynamic consent in the context of personal health data sharing through the MyHealthHub application. Their study highlights the opportunities dynamic consent provides for empowering users with personalized options, noting that most participants successfully completed all tasks independently and viewed the personalized options favourably. However, their study also examines the challenges of implementing digital consent systems, such as concerns around security, reliability, and the need for strong authentication mechanisms to protect privacy.

(Verreydt et al. 2021) conducted a systematic review of security and privacy challenges in electronic consent implementations. Their study categorized literature into two main areas: one focusing on representing and enforcing consent preferences electronically, and the other on implementing e-consent in data-sharing systems. The study also highlighted that centralized systems often lack transparency, while distributed solutions like blockchain face confidentiality challenges. As a result, no solution fully addresses all information security principles, with the gap attributed to the lack of universally agreed-upon requirements. (Kakarlapudi et al. 2021) conducted a systematic review on using blockchain technology for managing consent and personal data in digital environments. By reviewing various applications of blockchain in consent models, their study identified both advantages, such as providing users with a clear and auditable record of consent, and challenges, including scalability and integration with existing systems. (Budin-Ljøsne et al. 2017) investigated how dynamic consent can address challenges in modern biomedical research, particularly participant recruitment, informed consent, and long-term engagement in a rapidly evolving environment. Their workshop highlighted the potential of dynamic consent to improve communication between researchers and participants, support cross-border data sharing, and bring economic efficiencies to research management.

While these studies provide valuable insights into the application of dynamic consent, they do not provide a comprehensive overview of the dynamic consent landscape through a SLR. They also do not analyze dynamic consent across various application domains and target groups, nor do they focus on key aspects such as privacy, trust, transparency, user control, and the core components of the consent management process. Beyond academic research, several practitioner-led initiatives have also explored human-centric and dynamic consent approaches. (MyData. 2025) initiative advocates for human-centric personal data management. This initiative has actively contributed to frameworks such as the GovStack initiative, which promotes digital government architectures supporting user-driven consent mechanisms. Similarly, (Prometheus-X. 2025) works on decentralized and interoperable consent management frameworks to enhance data sovereignty and transparency in data sharing ecosystems. (Solid Project. 2025) is another relevant initiative that focuses on decentralized data storage, enabling users to have greater control over their personal data and consent preferences. These initiatives reflect ongoing efforts to address practical challenges in

consent management, including issues of usability, security, and standardization.

4. Research Methodology

For our SLR protocol development, we followed to the procedures and guidelines established by (Kitchenham et al. 2009) and (Cooper et al. 2018). This process involved outlining the Research Question (RQ), formulating a search strategy, establishing inclusion and exclusion criteria for studies, and detailing the methods for data extraction. The primary aim of this SLR is to address the following **RQ**: How can dynamic consent be framed to balance privacy, trust, safety, and risk management in Human-Computer Interaction?

To address this main RQ, we have formulated the following sub-questions (SQs):

SQ1. What is the current landscape of dynamic consent, including application domains, target groups, and the aspects of privacy, trust, transparency, and user control addressed?

SQ2. Which high-level elements and sub-elements of digital consent management are involved in dynamic consent?

The selection of literature related to the landscape of dynamic consent follows a two-stage process:

(i) We formulated a search string using keywords relevant to our topic. This string is employed to conduct comprehensive and systematic searches across the selected scientific databases:

Search String: ((("Dynamic Consent") OR ("Adaptive Consent")) AND (("Privacy") OR ("Trust") OR ("Transparency") OR ("User Control")))

The keywords were categorized into two groups to represent the core components of this study: the primary concept (i.e., dynamic or adaptive consent), and the aspects potentially addressed by dynamic consent (i.e., privacy, trust, transparency, or user control).

(ii) We conducted searches across several scientific databases, including ACM Digital Library, IEEE Xplore, ScienceDirect, SpringerLink, and Wiley. The literature considered for inclusion was published between 2019 and 2024, up to the search period. Our search process took place in October and November 2024. We followed the structured guidelines for systematic literature searching outlined by (Cooper et al. 2018), which include determining the individuals responsible for the search, defining the search objectives and scope, planning the search process, formulating the search strategy, selecting the appropriate scientific databases, conducting additional searches as required, organizing the collected references, and documenting the results of the search.

Inclusion Criteria (IC) for our SLR are:

IC1. Must be published in a journal, conference, or book chapters.

IC2. Published between 2019 and 2024, up to the search period.

IC3. Must address dynamic consent.

IC4. Must address at least one of the following aspects: privacy, trust, transparency, and user control.

Exclusion Criteria (EC) for our SLR are:

EC1. Studies published in languages other than English were excluded.

EC2. Studies that only provide basic information on dynamic consent were excluded.

EC3. Studies that address dynamic consent but do not focus on any aspects including privacy, trust, transparency, and user control were excluded.

5. Results

SQ1. What is the current landscape of dynamic consent, including application domains, target groups, and the aspects of privacy, trust, transparency, and user control addressed?

The search process identified 341 records across the following scientific databases: ACM Digital Library (n = 26), IEEE Xplore (n = 7), ScienceDirect (n = 63), SpringerLink (n = 197), and Wiley (n = 48). After removing duplicates, screening the abstract, title, keywords, and full papers based on our IC and EC, we selected 30 records for detailed analysis using our data extraction procedures. The list of papers on the current landscape of dynamic consent, based on our screening process, is shown in Table 1 and primarily addresses our **SQ1**.

Table 1 categorizes the identified studies by application domain. Notably, 27 out of the 30 studies focus on health-related applications, with an emphasis on dynamic consent in contexts such as health data sharing, clinical trials,

biobanking, and genomic research. Only 3 out of the 30 studies address generic or IoT-specific applications. The target groups in the studies predominantly include individuals participating in health research, such as patients, biobank participants, and users of wearable devices and mobile health sensors. For instance, (Lee et al. 2021) targeted individuals using wearables and mobile devices for health data sharing, while (Albanese et al. 2020) focused on participants in clinical trials. In addition, some studies addressed users of IoT devices (Pöhls et al. 2020), and participants in cross-enterprise data sharing (Zhang et al. 2022).

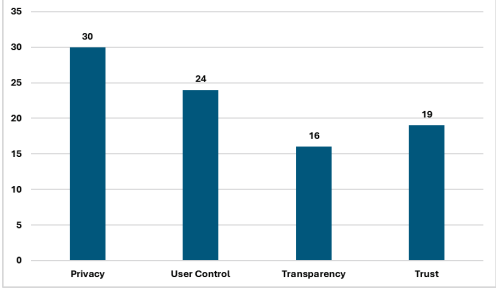

Fig. 1. Key Aspects of Dynamic Consent Addressed in the Identified Studies

Fig. 1 presents an analysis of the key aspects, privacy, user control, transparency, and trust, addressed in the identified studies on dynamic consent. The results show that privacy is the most frequently discussed aspect, appearing in all 30 studies, highlighting the critical importance of protecting user data in consent mechanisms. User control, highlighted in 24 out of the 30 studies, highlights the importance of empowering individuals to dynamically manage and modify their consent. In contrast, transparency (addressed in 16 out of 30 studies) and trust (addressed in 19 out of 30 studies) receive relatively less attention. This suggests that while privacy and control mechanisms are prioritized, there may be opportunities to enhance openness in consent processes and build stronger user confidence. For instance, (Alhajri et al. 2022) address all four aspects, demonstrating an effort to integrate a holistic approach to consent mechanisms that considers security, user control, transparency, and trust.

Table 1. Current Landscape of Dynamic Consent and Corresponding Application Domains

ID	Paper Title (Reference)	Application Domain
1	Blockchain-Integrated Deep Learning for Secure Health Data Sharing and Consent Management (Deepthika et al. 2024)	Health
2	Evaluation of CTRL: a web application for dynamic consent and engagement with individuals involved in a cardiovascular genetic disorders cohort (Haas et al. 2024)	Health
3	'CTRL': an online, Dynamic Consent and participant engagement platform working towards solving the complexities of consent in genomic research (Haas et al. 2024)	Health
4	ACE: A Consent-Embedded privacy-preserving search on genomic database (Jafarbeiki et al. 2024)	Health
5	Opportunities and challenges of a dynamic consent-based application: personalized options for personal health data sharing and utilization (Lee et al. 2024)	Health
6	PriviAware: Exploring Data Visualization and Dynamic Privacy Control Support for Data Collection in Mobile Sensing Research (Lee et al. 2024)	Health
7	Integrating Population-Based Biobanks: Catalyst for Advances in Precision Health (Lin et al. 2024)	Health
8	Exploring the Future of Informed Consent: Applying a Service Design Approach (McInnis et al. 2024)	Health
9	Distributed management of patient data-sharing informed consents for clinical research (Pham et al. 2024)	Health
10	Data Stewardship in Clinical Computer Security: Balancing Benefit and Burden in Participatory Systems (Tseng et al. 2024)	Health
11	Usability for Data Sovereignty - Evaluation of Privacy Risk Quantification Interfaces (Appenzeller et al. 2023)	Health
12	The Social Contract for Health and Wellness Data Sharing Needs a Trusted Standardized Consent (Brückner et al. 2023)	Health
13	Blockchain Based Dynamic Consent Management Systems for Enhancing Quality of Life for People with Disabilities (Khalid et al. 2023)	Health
14	Ensuring Electronic Health Record (EHR) Privacy using Zero Knowledge Proofs (ZKP) and Secure Encryption Schemes on Blockchain (Ranaweera et al. 2023)	Health
15	Blockchain-based Secure Storage and Management of Electronic Health Record using a Smart Card (Srivastava et al. 2023)	Health
16	A Blockchain-Based Consent Mechanism for Access to Fitness Data in the Healthcare Context (Alhajri et al. 2022)	Generic
17	Evaluation of a blockchain-based dynamic consent platform (METORY) in a decentralized and multicenter clinical trial using virtual drugs (Huh et al. 2022)	Health
18	A Blockchain-based platform for data management and sharing (Kumi et al. 2022)	Health
19	LUCE: A blockchain-based data sharing platform for monitoring data License accoUntability and CompliancE (Urovi et al. 2022)	Generic
20	Ten years of dynamic consent in the CHRIS study: informed consent as a dynamic process (Mascalzoni et al. 2022)	Health
21	Patient-centered cross-enterprise document sharing and dynamic consent framework using consortium blockchain and ciphertext-policy attribute-based encryption (Zhang et al. 2022)	Health
22	The practice of active patient involvement in rare disease research using ICT: experiences and lessons from the RUDY JAPAN project (Hamakawa et al. 2021)	Health
23	Dynamic Consent for Sensor-Driven Research (Lee et al. 2021)	Health
24	Dynamic consent management for clinical trials via private blockchain technology (Albanese et al. 2020)	Health
25	Dwarna: a blockchain solution for dynamic consent in biobanking (Mamo et al. 2020)	Health
26	Assessing the stability of biobank donor preferences regarding sample use: evidence supporting the value of dynamic consent (Pacyna et al. 2020)	Health
27	Dynamic Consent: Physical Switches and Feedback to Adjust Consent to IoT Data Collection (Pöhls et al. 2020)	IoT
28	Can dynamic consent facilitate the protection of biomedical big data in biobanking in Malaysia? (Abdul Aziz et al. 2019)	Health
29	French-style genetics v. 2.0: The "e-CohortE" project (Stoeklé et al. 2019)	Health
30	Why We Trust Dynamic Consent to Deliver on Privacy (Schuler Scott et al. 2019)	Generic

SQ2. Which high-level elements and sub-elements of digital consent management are involved in dynamic consent?

Some of the identified studies highlight "Identification and Authentication" as a fundamental component of dynamic consent. For instance, (Alhajri et al. 2022) emphasize the role of identification and authentication in dynamic consent. Their proposed system utilizes blockchain technology and smart contracts to authenticate users and ensure secure, tamper-proof consent transactions. When users provide consent, their identity is verified through cryptographic authentication mechanisms, ensuring that only authorized individuals can

grant, modify, or withdraw consent. The system also incorporates a regulatory authority to oversees the authentication process, preventing unauthorized access, and fraudulent consent modifications. By utilizing digital signatures, cryptographic hashing, and smart contract-based verification, their system enhances security, allowing users to reliably re-identify themselves and manage consent dynamically while complying with legal and regulatory requirements such as GDPR.

Core consent management is addressed in many of the identified studies. However, only one study specifically focuses on the user-facing transparency dashboard for communicating risks. (Appenzeller et al. 2023) addresses the HCI aspects of risk visualization within a user-facing transparency dashboard for consent management. Their study specifically investigates how users interpret and interact with privacy risk quantification scores and dynamic consent interfaces. Through usability testing and interface design variations, the study demonstrates how different visual representations of risk, such as traffic light indicators, Nutri-score style rankings, and factor-based explanations, can influence user understanding and consent decisions. Finally, portability management has received relatively less attention in the identified studies, despite its importance in enabling users to access and transfer their data.

6. Discussion: A Position on Balancing Privacy, Trust, Security, and Risk Communication for System Reliability

Based on our findings, only one study specifically addresses dynamic consent in the context of IoT (Pöhls et al. 2020). However, several healthcare studies also involve IoT devices. For example, patients wearing wearable devices, such as fitness trackers or sharing data through mobile health sensors are subject to dynamic consent mechanisms (Lee et al. 2021). These studies highlight the evolving integration of IoT technologies in domains such as healthcare, enabling real-time data collection. As IoT devices, such as wearables and mobile health sensors, become increasingly widespread, they support continuous monitoring and data sharing. This increasing use of IoT across sectors highlights the need for dynamic consent mechanisms that can adapt to the evolving landscape of data usage and privacy concerns.

Privacy, user control, transparency, and trust are key elements of dynamic consent. Some studies address all of these aspects (Deepthika et al. 2024), (Khalid et al. 2023), (Alhajri et al. 2022). However, security and risk management also need adequate attention in the context of dynamic consent, an area currently underexplored. While the security of dynamic consent platforms is considered in existing studies, the broader impact of security on privacy and the safety risks associated with privacy breaches have not been sufficiently explored. In IoT environments, where data is continuously collected, the privacy impact of each data point can vary depending on factors such as data sensitivity, security, safety, usage, and device interconnectivity. For instance, a wearable fitness tracker that collects sensitive health data such as heart rate and location can be vulnerable to security breaches. If compromised, unauthorized third parties could access personal health data, directly impacting user privacy.

On the other hand, implementing security measures, such as multi-factor authentication, can significantly reduce these risks. With stronger security, the privacy impact of the data decreases, as unauthorized access becomes more difficult. As these systems evolve, the risks to both privacy and security change, and safety risks become even more critical, especially when health is at stake. This is where the HCI aspects of the user-facing transparency dashboard become vital. Effective risk communication enables end-users make informed decisions, considering key factors such as privacy, user control, transparency, trust, safety, and security.

However, only one out of the 30 studies focused on HCI aspects of user-facing transparency dashboard. (Appenzeller et al. 2023) evaluated privacy risk quantification interfaces designed to support data sovereignty. Their study highlights the importance of providing users with clear, understandable privacy risk information, which helps them make informed decisions. However, it also lacks communication about safety and security risks. While users must be informed of safety and security risks that could affect privacy, it is crucial to avoid overwhelming them with excessive or overly complex information.

The challenge lies in effectively communicating both safety and security measures that protect users' data, while ensuring that the information remains accessible and understandable.

7. Conclusions and Future Work Directions

In this study, we conducted a SLR to explore the current landscape of dynamic consent, focusing on its application across different domains and key components of digital consent management. We identified 30 studies and analyzed how dynamic consent incorporates privacy, user control, transparency, and trust, and determined which aspects are addressed. Our findings highlight that while privacy and user control are commonly discussed in existing research, security and safety risks remain underexplored, particularly regarding their impact on privacy. Notably, only one study explicitly focused on the HCI aspects of user-facing transparency dashboards for risk communication, highlighting a significant gap. A key direction for future work is the development of HCI concepts that effectively communicate safety and security measures influencing privacy risks. By improving risk communication and user control through enhanced HCI design, greater trust in dynamic consent systems can be established.

References

Kaye, J. et al. (2015). "Dynamic consent: a patient interface for twenty-first century research networks," European journal of human genetics, vol. 23.

Thapa, C. and S. Camtepe (2021). "Precision health data: Requirements, challenges and existing techniques for data security and privacy," Computers in biology and medicine, vol. 129.

Merlec, M. M. et al. (2021). "A smart contract-based dynamic consent management system for personal data usage under GDPR," Sensors, vol. 21, no. 23.

Schuler Scott, A. (2022). "Dynamic consent: a mechanism for engagement," University of Oxford.

Lähteenoja, V. et al. (2024). "The landscape of consent management tools – a data altruism perspective".

Lay, W. et al. (2025). "A rapid review of the benefits and challenges of dynamic consent," Research Ethics, vol. 21, pp. 180 – 202.

Lee, A. R. et al. (2024). "Opportunities and challenges of a dynamic consent-based application: personalized options for personal health data sharing and utilization," BMC Medical Ethics, vol. 25.

Verreydt, S. et al. (2021). "Security and privacy requirements for electronic consent: a systematic literature review," ACM Transactions on Computing for Healthcare, vol. 2, no. 2, pp. 1 – 24.

Kakarlapudi, P. V. et al. (2021). "A systematic review of blockchain for consent management," Healthcare, MDPI.

Budin-Ljøsne, I. et al. (2017). "Dynamic consent: a potential solution to some of the challenges of modern biomedical research," BMC medical ethics, vol. 18.

MyData. (2025). "MyData – About." [Online]. Available: https://mydata.org/

Prometheus-X. (2025). "Prometheus-X: Building Blocks," [Online]. Available: https://prometheus-x.org/building-blocks/

Solid Project. (2025). "Solid Project – About Solid," [Online]. Available: https://solidproject.org/about

Kitchenham, B. et al. (2009). "Systematic literature reviews in software engineering – a systematic literature review," Information and software technology, pp. 7 – 15.

Cooper, C. et al. (2018), "Defining the process to literature searching in systematic reviews: a literature review of guidance and supporting studies," BMC medical research methodology, vol. 18, pp. 1–14.

Deepthika, K. et al. (2024). "Blockchain-Integrated Deep Learning for Secure Health Data Sharing and Consent Management," Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), IEEE, pp. 101 – 106.

Haas, M. A. et al. (2024). "Evaluation of CTRL: a web application for dynamic consent and engagement with individuals involved in a cardiovascular genetic disorders cohort," European Journal of Human Genetics, vol. 32.

Jafarbeiki, S. et al. (2024). "ACE: A Consent-Embedded privacy-preserving search on genomic database," Heliyon, vol. 10, no. 8.

Lee, H. et al. (2024). "PriviAware: Exploring Data Visualization and Dynamic Privacy Control Support for Data Collection in Mobile Sensing Research," in Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1 – 17.

Lin, J.-C. et al. (2024). "Integrating population-based biobanks: Catalyst for advances in precision health," Computational and Structural Biotechnology Journal, vol. 24, pp. 690 – 698.

McInnis, B. J. et al. (2024). "Exploring the Future of Informed Consent: Applying a Service Design Approach," Proceedings of the ACM on Human-Computer Interaction, vol. 8.

Pham, A. et al. (2024). "Distributed management of patient data-sharing informed consents for clinical research," Computers in biology and medicine, vol. 180.

Tseng, E. et al. (2024). "Data Stewardship in Clinical Computer Security: Balancing Benefit and Burden in

Participatory Systems," Proceedings of the ACM on Human-Computer Interaction, vol. 8, pp. 1 – 29.
Appenzeller, A. et al. (2023). "Usability for Data Sovereignty-Evaluation of Privacy Risk Quantification Interfaces," Proceedings of the 16th International Conference on PErvasive Technologies Related to Assistive Environments, pp. 206 – 214.
Brückner, S. et al. (2023). "The social contract for health and wellness data sharing needs a trusted standardized consent," Mayo Clinic Proceedings: Digital Health, vol. 1, no. 4, pp. 527 – 533.
Khalid, M. I. et al. (2023). "Blockchain Based Dynamic Consent Management Systems for Enhancing Quality of Life for People with Disabilities," IEEE International Smart Cities Conference (ISC2).
Ranaweera, T. et al. (2023). "Ensuring Electronic Health Record (EHR) Privacy using Zero Knowledge Proofs (ZKP) and Secure Encryption Schemes on Blockchain," 5th International Conference on Advancements in Computing (ICAC), pp. 792 – 797.
Srivastava, I. et al. (2023). "Blockchain-based Secure Storage and Management of Electronic Health Record using a Smart Card," 5th International Conference on Recent Advances in Information Technology (RAIT).
Alhajri, M. et al. (2022). "A blockchain-based consent mechanism for access to fitness data in the healthcare context," IEEE Access, vol. 10, pp. 22960 – 22979.
Huh, K. Y. et al. (2022). "Evaluation of a blockchain-based dynamic consent platform (METORY) in a decentralized and multicenter clinical trial using virtual drugs," Clinical and Translational Science, vol. 15, no. 5, pp. 1257 – 1268.
Kumi, S. et al. (2022). "A Blockchain-based platform for data management and sharing," Procedia Computer Science, vol. 203, pp. 95 – 102.
Urovi, V. et al. (2022). "Luce: A blockchain-based data sharing platform for monitoring data license accountability and compliance," Blockchain: Research and Applications, vol. 3.
Mascalzoni et al. (2022). "Ten years of dynamic consent in the CHRIS study: informed consent as a dynamic process," European Journal of Human Genetics, vol. 30.
Zhang, L. et al. (2022) "Patient-centered cross-enterprise document sharing and dynamic consent framework using consortium blockchain and ciphertext-policy attribute-based encryption," Proceedings of the 19th International Conference on Computing Frontiers.
Hamakawa, N. et al. (2021). "The practice of active patient involvement in rare disease research using ICT: experiences and lessons from the RUDY JAPAN project," Research Involvement and Engagement, vol. 7, pp. 1 – 15.
Lee, H. et al. (2021). "Dynamic consent for sensor-driven research," Thirteenth International Conference on Mobile Computing and Ubiquitous Network, IEEE.
Albanese, G. et al. (2020). "Dynamic consent management for clinical trials via private blockchain technology," Journal of ambient intelligence and humanized computing, vol. 11.
Mamo, N. et al. (2020). "Dwarna: a blockchain solution for dynamic consent in biobanking," European Journal of Human Genetics, vol. 28, no. 5, pp. 609 – 626.
Pacyna, J. E. et al. (2020). "Assessing the stability of biobank donor preferences regarding sample use: evidence supporting the value of dynamic consent," European Journal of Human Genetics, vol. 28.
Pöhls, H. C. et al. (2020). "Dynamic consent: physical switches and feedback to adjust consent to IoT data collection," 22nd HCI International Conference.
Abdul Aziz, M. F. et al. (2019). "Can dynamic consent facilitate the protection of biomedical big data in biobanking in Malaysia?," Asian Bioethics Review, vol. 11, pp. 209 – 222.
Stoeklé, H.-C. et al. (2019). "French-style genetics v. 2.0: The 'e-CohortE' project," Clinical Genetics, vol. 96.
Schuler Scott, A. et al. (2019). "Why we trust dynamic consent to deliver on privacy," IFIPTM 2019, pp. 28 – 38.