# Modernizing Informed Consent for Ubiquitous Personal Health Information Collection: A Blockchain Dynamic Informed Consent Platform for Public Health Research

by

Pedro Augusto Da Silva E Souza Miranda

A thesis

presented to the University of Waterloo

in fulfillment of the

thesis requirement for the degree of

Doctor of Philosophy

in

Public Health Sciences

Waterloo, Ontario, Canada, 2026

© Pedro Augusto Da Silva E Souza Miranda 2026

## Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

| | |
|---|---|
| External Examiner | Dr. Maria Lindén<br>Associate Professor<br>Department of Computer Science and Engineering<br>Mälardalen University |
| Supervisor | Dr. Plinio P. Morita<br>Associate Professor<br>School of Public Health Sciences<br>University of Waterloo |
| Internal Member | Dr. James Wallace<br>Professor<br>School of Public Health Sciences<br>University of Waterloo |
| Internal-External Member | Dr. Maura R. Grossman<br>Research Professor<br>David R. Cheriton School of Computer Science<br>University of Waterloo |
| Internal-External Member | Dr. Adam Molnar<br>Associate Professor<br>Sociology and Legal Studies<br>University of Waterloo |

## Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners. I understand that my thesis may be made electronically available to the public.

## Statement of Contributions

Portions of this thesis draw on publications and collaborative research completed during this doctoral program. The publications and related outputs most directly connected to the thesis are: Pedro, P. A., & Morita, P. P. (2022), A Proposed Personal Data Sovereignty Inter-Organizational Governance Framework for Public Health Research; Miranda, P. A., Kaur, J., & Morita, P. (2023), UbiSecE: UbiLab's Secure Cloud Environment for Public Health Research in Microsoft Azure; and Velmovitsky, P. E., Souza Miranda, P. A. D. S. E., Vaillancourt, H., Donovska, T., Teague, J., & Morita, P. P. (2020), A Blockchain-Based Consent Platform for Active Assisted Living: Modeling Study and Conceptual Framework.

For the thesis-specific work, I led the conceptualization of the dynamic informed consent problem, the governance-framework development, the Consentio platform design and implementation, the evaluation design, the analysis, and the writing and integration of the thesis manuscript. Co-authors, supervisors, committee members, and collaborators contributed through supervision, conceptual feedback, infrastructure support, methodological advice, manuscript review, and revision guidance. Any material derived from collaborative work has been rewritten, integrated, and extended for the purposes of this thesis.

Finally, three additional publications are scheduled for Fall 2026. The first will be a journal article detailing the development of the data governance framework (Section 6). The second will describe the methodology outlined in Section 7, which involves mapping the data governance framework into a traceability matrix aligned with the software requirements for developing the dynamic informed consent management platform. The third will present the results of a multi-method user evaluation study of the developed platform (Sections 8 & 9), including its implications for adoption, necessary improvements, and future steps required to advance the work.

# Abstract

Public health research is increasingly dependent on ubiquitous collections of personal health information (PHI) and personal data drawn from wearable sensors, electronic records, and connected devices. Traditional informed-consent processes, often paper-based and one-time agreements, cannot meet the demands of real-time data flows, cross-institutional sharing, and evolving regulatory requirements. This thesis proposes and tests a novel approach to dynamic informed consent, grounded in data governance theory and implemented through tamper-evident ledger technologies.

First, it develops an Inter-Organizational Data Governance (IODG) framework tailored for public-health research. Using the Governance Analytical Framework, the thesis maps actors, social norms, and transaction types, and allocates decision rights and accountability to researchers, data custodians, regulators, and data subjects. The framework emphasizes personal data sovereignty and prescribes a phased implementation, with validation, endorsement, and machine-readable policies to make PHI sharing lawful, transparent, and auditable.

Second, the thesis translates this framework into the Consentio platform ("*I consent*", in Latin), a web-based dynamic consent platform. Governance clauses are decomposed into formal requirements and encoded as use cases, class and state diagrams; propositional logic invariants enforce legal states; Angular route guards and validators prevent unauthorized actions; and a permissioned ledger records immutable, cryptographically verifiable receipts for approvals, consent, and data-sharing events.

Third, a mixed-methods user evaluation assesses the platform. Ten participants (five researchers and five data subjects) reported high usability (global PSSUQ mean = 1.82 on a 1–7 scale), moderate to high digital skills and strong satisfaction, yielding a favorable Net Promoter Score. A reflexive thematic analysis of interviews and open-ended feedback revealed eight themes: participants valued granular control and centralized dashboards but sought clearer explanations of revocation limits and ledger security;

progressive disclosure balanced efficiency and comprehension; and researchers desired customization, improved notifications, and audit-ready reporting.

The findings suggest that coupling principled governance, formal system design and ledger-backed auditability can modernize informed-consent management for data-intensive public-health research, enhancing trust, autonomy and regulatory compliance. Future work should extend the framework to more diverse populations, refine interface elements for error recovery and ledger explanation, and evaluate scalability and interoperability across varied research domains.

## Acknowledgements

I would like to acknowledge the organizations and communities that enabled this work. Financial and in-kind support from MITACS and the CSA Group enabled key stages of the research, including time to iterate on platform design, implementation, and evaluation. I am also grateful to the Université de Technologie de Compiègne for its institutional support and collegial welcome, which strengthened the international dimension of this thesis and broadened the perspectives that informed the work.

This thesis was developed within the Ubiquitous Health Technology Lab (UbiLab), and I am deeply grateful for the environment it provided, where rigorous research and practical engineering could coexist meaningfully. I am especially grateful to my colleagues at UbiLab for their feedback, problem-solving conversations, and day-to-day support, which shaped both the quality of the research and the resilience needed to complete it.

Finally, I would like to acknowledge the many informal contributions that rarely appear in methods sections but matter profoundly in practice, including peers who reviewed drafts, collaborators who offered timely advice, and friends and family who provided patience and encouragement throughout the doctorate.

# Dedication

To my Father, Antonio Carlos Miranda, who devoted his life to medicine, working from nine to nine through most of my childhood to provide for us and becoming one of Brazil's leading proctologists–oncologists; and my Mother, Luiza Cristina Da Silva E Souza Miranda, an extraordinary physician and urgent-care team leader who balanced clinical leadership with the demands of motherhood. Together, they never gave up on me; even in the hardest moments, they met me with unwavering care and a steady insistence on growth. Their sacrifices, discipline, and love made this work possible, and I carry their example into every page.

To my lovely wife, Bruna Miranda, who loved and believed in me from day one and shared our audacious dream of building a life in Canada. She sustained this PhD emotionally and financially and met every headwind with quiet strength and capability. I am profoundly and permanently grateful for her love and partnership.

To my advisor, Plinio Morita, who welcomed me into this PhD program and supported it with both material and moral generosity. His guidance optimistic yet unflinchingly realistic approach sharpened the ideas, steadied the timelines, and made completion possible. I am deeply thankful to have learned under his mentorship.

To Professor Carlos Lucena, who gave me the chance to reset my academic trajectory when my undergraduate record bore the weight of personal hardship. His confidence in me at LES-PUC-Rio revived my scholarly vocation and opened the path I continue to walk.

To Andrew Costa, my undergraduate advisor, whose early encouragement and clear-eyed counsel first awakened my interest in research and guided me toward graduate study.

To Marx Vianna, whose friendship and steady guidance throughout my master's were essential to my progress and success.

To André Lucena, who stood by my work from the end of my undergraduate years through my master's, whose support was decisive in my admission to this PhD, and who continues to champion my efforts today.

To my psychiatrist, Dr. Ghuman, whose care over the past two years equipped me with the tools to face and manage my mental health challenges; without that care, this dissertation would not exist.

To Arlene Oetomo, whose friendship, candor, and timely advice kept me moving when it would have been easier to stop.

# Table of Contents

List of Figures ..... xiv

List of Tables ..... xv

List of Abbreviations ..... xvii

Quote ..... xviii

1 Introduction ..... 1

1.1 Thesis Logic Map ..... 3

1.2 Problem Statement ..... 6

2 Background ..... 9

2.1 Challenges to Data Collection in Public Health Research ..... 9

2.2 Challenges of Bigdata Analysis ..... 10

2.3 Traditional Informed Consent Form Limitations ..... 11

2.4 Dynamic Informed Consent ..... 12

2.5 Dynamic Informed Consent Management Solutions ..... 13

2.6 Data Governance ..... 13

2.7 Data Governance Models ..... 14

2.8 Ledger Technologies ..... 14

2.9 Challenges of Big Data Collection for Public Health Research ..... 17

3 Motivation ..... 19

3.1 From Medical Oaths to Formal Codes ..... 19

3.2 Twentieth-Century Ethical Milestones ..... 20

3.3 Contemporary Challenges And Innovations ..... 21

3.4 Chronic Patterns of Unethical Research ..... 22

3.5 Beecher's 1966 Exposé and the Continued Violations of Informed Consent in the Modern Era 24

4 Work Completed ..... 27

5 Thesis Organization ..... 30

6 An Inter-Organizational Personal Data Sovereignty Governance Framework for Public Health Research 31

6.1 Introduction ..... 31

6.2 Public Health Research Access to Personal Health Information ..... 32

6.3 Objectives ..... 33

6.4 Background ..... 34

6.5 Data Governance Requirements for Public Health Research ..... 38

6.6 Methods: Application of the Governance Analytical Framework (GAF) ..... 43

6.7 Defining GAF Components for the Public Health Domain ..... 45

6.8 Results ..... 46

6.9 Mapping of Public Health Research Domain's Transactions (GAF Transactions) ..... 54

6.10 Personal Data Sovereignty Inter-Organizational Data Governance Model for Public Health Research 59

6.11 Research Questions ..... 61

6.12 Discussion ..... 63

6.13 Limitations and Boundary Conditions ..... 66

6.14 Pathways to Implementation ..... 66

6.15 Relevance ..... 66

6.16 Conclusion ..... 67

7 Translating Data Governance Concepts into a Working Dynamic Informed Consent Management Platform ..... 69

7.1 Introduction ..... 69

7.2 Motivation ..... 69

7.3 Specific Aims ..... 70

7.4 Methods ..... 72

7.5 Integration Plan ..... 76

7.6 Actor Alignment ..... 76

7.7 Core Use Cases and their Governance Obligations ..... 77

7.8 Governance-to-Implementation Traceability Matrix ..... 78

7.9 Consentio Platform's Class Diagram ..... 80

7.10 State Diagrams and Governance Alignment ..... 82

7.11 Formalized Logic and Constraints for Consentio ..... 91

7.12 Entities and Propositional Variables ..... 93

7.13 Constraints by Entity ..... 95

7.14 Operationalizing Consent Governance: Interfaces and Functionalities ..... 96

7.15 Results and Implementation Summary ..... 101

7.16 Limitations ..... 102

7.17 Discussion ..... 103

7.18 Conclusion ..... 105

8 Quantitative Assessment of Consentio Dynamic Informed Consent Platform Based on Participants' Surveys ..... 106

8.1 Introduction ..... 106

8.2 Research Questions ..... 107

8.3 Methods ..... 109

8.4 Survey Instruments ..... 113

8.5 Data Processing and Analysis ..... 117

8.6 Results ..... 118

8.7 Discussion ..... 125

8.8 Conclusion ..... 129

9 Reflexive Thematic Analysis of Consentio Dynamic Informed Consent Platform Based on Participants' Interviews and Surveys' Discursive Answers ..... 130

9.1 Introduction ..... 130

9.2 Epistemic Stance and Methodology ..... 130

9.3 Reflexive Thematic Analysis ..... 133

9.4 Interviews and Data Sources ..... 135

9.5 Research Questions Strategies ..... 138

9.6 Analytic Orientation and Quality Procedures ..... 143

9.7 Results: Themes Across Participants and Researchers ..... 143

9.8 Cross-Theme Tensions and Synthesis ..... 150

9.9 Design Implications and Recommendations Summary ..... 152

9.10 Discussion ..... 153

9.11 Which Aspects of Usability Support or Threaten Informed Consent ..... 155

9.12 Conclusion ..... 157

10 Summary of Design Recommendations for a Governance Guided, Blockchain-based, Tailored for Public Health Research That Leverages Personal Health Information Dynamic Informed Consent Management Platform ..... 162

10.1 Introduction ..... 162

10.2 Aligning User Experiences with the Broader Research Context ..... 162

11 Limitations ..... 170

12 Overarching Conclusions ..... 172

13 Thesis Contributions ..... 174

References ..... 179

Appendix A ..... 215

Appendix B ..... 219

Appendix C ..... 226

Appendix D ..... 231

Appendix E ..... 234

Appendix F ..... 268

## List of Figures

Figure 1 - Relationship between public health research principles and goals and IT infrastructure. ..... 36

Figure 2 - ISO/IEC 38500 conceptual model..... 41

Figure 3 - Independent and dependent variables of the public health research domain based on the GAF. ..... 47

Figure 4 - GAF diagram of data governance for public health research..... 48

Figure 5 - Personal Data Sovereignty Governance Framework for Public Health Research. ..... 57

Figure 6 - Personal Data Sovereignty Inter-Organizational Data Governance Model for Public Health Research ..... 60

Figure 7 - Platform class diagram..... 81

Figure 8 - Researcher State Diagram. ..... 83

Figure 9 - Dynamic Informed Consent Form State Diagram..... 85

Figure 10 - Auditor State Diagram. ..... 86

Figure 11 - Participant State Diagram..... 87

Figure 12 - Principal Investigator (PI) State Diagram. ..... 88

Figure 13 - Study Approval State Diagram. ..... 90

Figure 14 - Consentio participant and researcher interface workflows. ..... 99

Figure 15 - Reflexive Thematic Analysis workflow diagram..... 135

Figure 16 - Relationship between themes. ..... 152

Figure 17 - Use case diagram of platform users. ..... 220

# List of Tables

Table 1 - Brief history of informed consent. 23

Table 2 - Beecher's examples of informed consent violations (1966). 25

Table 3 - Modern examples of informed consent violations. 25

Table 4 - Data governance models mapped by (Micheli et al., 2020b). 39

Table 5 - Governance actors and social norms in public health research. 50

Table 6 - Social norms legend for public health research governance. 51

Table 7 - Actor-to-actor governance transaction typology. 55

Table 8 - Illustrative governance transaction scenarios. 56

Table 9 - Actor alignment table. 77

Table 11 - GAF Mapping. 82

Table 12 - Propositional logic variables and meaning. 94

Table 13 - Survey instrument details. 116

Table 14 - Demographics survey results. 119

Table 15 - PSSUQ Results. 120

Table 16 - ISS results. 121

Table 17 - CUSE survey results. 123

Table 18 - CSAT survey results. 124

Table 19 - Net Promoter Score survey results. 125

Table 20 - Recurrent excerpts used for theme mapping. 132

Table 21 - Participants' demographics. 137

Table 22 - Subthemes and Representative Codes. 151

Table 23 - Mapping of Section 6's challenges into themes. 164

Table 24 - Cross-analysis of Section 7 design features and user feedback. 165

Table 25 - Cross-section synthesis of thesis findings. 168

Table 26 - Technology mapped for the informed consent management platform. ..... 176

Table 27 - Dynamic Consent Management Platform Requirements. ..... 218

Table 28 - Catalogue of all use-cases that appear in Section 7 UML diagram. ..... 222

Table 29 - Governance-to-implementation traceability matrix. ..... 268

## List of Abbreviations

1. AODA - Accessibility for Ontarians with Disabilities Act
2. API - Application Programming Interface
3. CCPA - California Consumer Privacy Act
4. CSAT - Customer Satisfaction
5. CUSE - Computer User Self-Efficacy
6. DC/DIC - Dynamic Consent / Dynamic Informed Consent
7. DG - Data Governance
8. DSA - Data Sharing Agreement
9. GAF - Governance Analytical Framework
10. GDPR - General Data Protection Regulation
11. IC - Informed Consent
12. IODG - Inter-Organizational Data Governance
13. IRB - Institutional Review Board
14. ISS - Internet Skills Scale
15. NPS - Net Promoter Score
16. PDS - Personal Data Sovereignty
17. PDSG - Personal Data Sovereignty Governance
18. PHI - Personal Health Information
19. PI - Principal Investigator
20. PII - Personal Identifiable Information
21. PIPEDA - Personal Information Protection and Electronic Documents Act
22. PSSUQ - Post-Study System Usability Questionnaire
23. RBAC - Role-Based Access Control
24. RQ - Research Question
25. RTA - Reflexive Thematic Analysis
26. TCPS2 - Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans
27. TIC - Traditional Informed Consent
28. UI - User Interface
29. UX - User Experience
30. WCAG - Web Content Accessibility Guidelines

## Quote

I’ve always been a relentless dreamer of possible futures; for twenty-five years, ADHD and PTSD kept me in a loop of bold beginnings and stalled middles. Finishing this thesis is proof that seeking help for my mental health broke the procrastination loop—and that I can see future innovations to the end.

— Pedro Augusto Da Silva E Souza Miranda

# 1 Introduction

Public health research is increasingly shaped by streams of personal data generated by wearable sensors, smartphone applications, smart home devices and patient portals. These technologies translate daily behaviours and physiological signals into analyzable digital footprints, enabling continuous monitoring and proactive health management (Zyskind et al., 2015). This transformation creates extraordinary opportunities to design more precise, timely, and equitable interventions, but it also amplifies an old problem: how to secure, maintain, and evidence valid informed consent when data sources are numerous, data uses evolve, and stakeholders span institutions and sectors. In this milieu, consent cannot be reduced to a signed page in a file. It is the living governance mechanism that connects data subjects, researchers, custodians, and regulators across time and technological change (Grady et al., 2017; O'Neill, 2003; Sugarman et al., 2005).

Contemporary public health research demands a rethinking of informed consent as an ongoing, participant-centred process rather than a single administrative event. As data collection and reuse increasingly span institutions, technologies, and time, consent must be supported by clear governance structures and digital systems capable of maintaining transparency, accountability, and trust.

Consent matters because it concretizes respect for persons, beneficence, and justice, the triad crystallized in the Belmont Report and echoed in later guidance by making participation voluntary, informed, and revocable as the risks and purposes of research evolve (Hiroyuki Nagai et al., 2022). A generation of scholarship has shown that when consent practices are treated as one-time, document-centric transactions, participants are often overwhelmed by legalistic prose, uncertainties about data reuse, and limited opportunities to revisit decisions (Bester et al., 2016; O'Neill, 2003; Sugarman et al., 2005). The resulting harms are not merely theoretical. Historical cases, most notoriously the U.S. Public Health Service study at Tuskegee, demonstrate how weak consent practices magnify structural inequities and corrode public trust (Brandt, 1978; Kerpel-Fronius et al., 2018). Contemporary data-driven health research poses

analogous hazards: permissions granted “up front” are stretched to cover unforeseen secondary uses; opaque algorithms entrench disparities; and data flows outpace mechanisms for oversight or participant agency (Obermeyer et al., 2019). If public health is to leverage ubiquitous personal health information (PHI) legitimately, consent must become more legible, dynamic, and auditable to non-experts and experts alike.

At the same time, the technical landscape of public health research has undergone profound changes. Big data infrastructures aggregate high-volume, high-velocity, and high-variety streams across organizational boundaries, calling for methods and governance that are different in kind, not degree(De Mauro et al., 2016; Demchenko et al., 2014). Mobile and wearable devices now generate behavioural and physiological traces at a population scale, enabling novel forms of monitoring and evaluation but also raising persistent concerns about data quality, interoperability, and re-identification risk (Cai & Zhu, 2015; Khoury & Ioannidis, 2014; Narayanan & Shmatikov, 2006, 2008). In this context, consent is inseparable from data governance: it is the rule-bound mechanism through which roles, duties, approvals, and rights to withdraw are expressed and enforced across heterogeneous systems and organizations (Marina Micheli et al., 2020). Without such an integrated approach, research remains either underpowered because recruitment and re-consent are costly or overexposed, because secondary uses multiply without commensurate transparency or control.

This thesis responds to that dual problem: the ethical requirement for meaningful, ongoing consent, and the practical requirement to implement that consent across inter-organizational data ecosystems. It advances a governance-to-platform pathway anchored in two complementary commitments. The first is methodological and normative: consent must be re-cast as a dynamic, participant-centred relationship rather than a static artifact, aligning with work on “dynamic consent” that emphasizes continuous communication, granular permissions, and re-contact (Budin-Ljøsne et al., 2017; Prinsen, 2024; Scott et al., 2018; Stein & Terry, 2013). The second is institutional and technical: because public health research typically spans organizations universities, health systems, private custodians, and regulators consent needs an explicit data

governance framework that defines actors, nodal decision points, social norms, and transaction types, coupled to infrastructure that can evidence compliance and propagate revocation in near-real time (Aeberhard & Rist, 2011; Marina Micheli et al., 2020; Pedro & Morita, 2022).

This thesis argues that dynamic informed consent for public health research must be treated as a governance problem and a software implementation problem at the same time. It contributes (1) an inter-organizational personal data sovereignty governance framework for PHI-based public health research, (2) the Consentio platform as a working translation of that framework into enforceable workflows and audit records, and (3) a mixed-methods evaluation showing how users experience control, transparency, usability, and trust in the platform. The central claim is that consent becomes meaningful only when participant agency, institutional accountability, and technical enforcement are designed together.

## 1.1 Thesis Logic Map

To make the thesis structure easier to follow, the detailed aims and section-level research questions are subordinate to three thesis-level questions. Research Question 1: What governance framework is needed for PHI-based public health research? Chapters 1 through 6 answer this question by moving from the problem of traditional informed consent to an inter-organizational personal data sovereignty governance framework. Research Question 2: How can that framework be translated into a working dynamic consent platform? Chapter 7 answers this question by mapping governance obligations to Consentio workflows, state controls, role-based access, and audit records. Research Question 3: How do researchers and participants experience the resulting platform? Chapters 8 through 10 answer this question through quantitative usability measures, qualitative thematic analysis, and synthesis of design implications.

The thesis is organized around a single governance-to-platform-to-evaluation arc: Section 6 develops the governance framework, Section 7 implements it in Consentio, and Sections 8 and 9 evaluate how users experience the resulting consent model. Section 10 then synthesizes design implications and connects the evaluation findings back to the framework.

Dynamic consent has emerged over the last decade as a pragmatic response to the limitations of traditional, paper-based consent (Grady et al., 2017; Kaye et al., 2015a). Rather than treating consent as a moment at enrolment, dynamic consent treats it as a dialogue mediated by digital tools: participants can view and revise preferences; researchers can request re-consent when protocols evolve; and both parties can audit what was agreed and when (Budin-Ljøsne et al., 2017; Prinsen, 2024). Evidence from biobanking and networked research shows that such models can increase understanding, trust, and willingness to participate, especially when interfaces are designed to minimize cognitive load and support layered disclosure (Budin-Ljøsne et al., 2017; Stein & Terry, 2013). Yet dynamic consent is not merely a "better form." It expands the unit of analysis from the page to the socio-technical system. That expansion raises concrete implementation questions: How are roles and duties encoded so that approvals are gate-checked at runtime? How is withdrawal enforced across data processors who are not co-located? How do auditors verify that a re-consent was obtained before a new data use? Those questions are governance questions before they are programming ones.

Data governance provides the institutional scaffolding for answering them. In public health research, governance clarifies who is responsible for what, under which norms, and with what accountability when data is accessed, linked, or shared (Marina Micheli et al., 2020). The Governance Analytical Framework (GAF) offers a tractable way to map this terrain by identifying the collective problem (e.g., enabling trustworthy data sharing), the actors involved (participants, researchers, ethics boards, custodians, regulators), the social norms in play (e.g., respect for autonomy, reciprocity), the nodal points where decisions are made (approval, enrolment, re-consent, withdrawal, data release), and the types of transactions that may be directive or negotiated (Aeberhard & Rist, 2011; Hufty, 2008). In parallel, the Personal Data Sovereignty (PDS) stance positions the data subject as a first-class actor whose agency is realized not only through "notice and choice" but through system behaviour that enforces decisions and makes them auditable (Pedro & Morita, 2022; Velmovitsky et al., 2020). Taken together, these perspectives argue that consent cannot be reliable unless governance is explicit and enacted.

This governance emphasis is not abstract. It responds directly to the operational realities of modern public health. Agencies and researchers increasingly rely on data that they do not directly generate or fully control, such as electronic health records, insurer claims, app telemetry, and sensor data, while remaining accountable for privacy, fairness, and public legitimacy (Government of Canada, 2019b; Khoury & Ioannidis, 2014). Data quality varies across sources; legal bases vary across jurisdictions; and the same data point may be processed by multiple parties for different purposes across time (Cai & Zhu, 2015; Martin-Sanchez et al., 2017). In this landscape, consent must function as a portable authorization with a verifiable history: an enrolment, a re-consent tied to a protocol change, a withdrawal with propagation duties that cut across organizational boundaries. The platform described in this thesis, Consentio, was designed to operationalize that portability by binding governance duties to application workflows and generating a tamper-evident audit trail of consent state changes that relevant parties can verify.

A natural concern is whether adding technology to a problem that is already ethical and social risks formalizing the wrong things. The position taken here is cautious but affirmative: digital infrastructure can support good governance when it is built to enforce, not replace, ethical predicates. Private, permissioned ledger technologies are one way to instantiate that enforcement because they excel at producing shared, time-stamped, tamper-evident records without disclosing sensitive content on-chain (Androulaki et al., 2018a; Benchoufi & Ravaud, 2017a; Jones et al., 2019). In a consent context, a ledger can maintain an immutable sequence of consent events: enroll, amend, withdraw, while off-chain services manage content (e.g., the form itself) under conventional security controls. Smart contracts can encode minimal, auditable predicates. For example, a re-analysis transaction is endorsable only if a matching re-consent event exists after a protocol amendment; a data release is endorsable only if no withdrawal supersedes the last positive consent (Androulaki et al., 2018a). Distributing endorsement across organizations, e.g., requiring an ethics board peer to endorse the correct ledger policy, can make governance participation unavoidable rather than aspirational. Importantly, this thesis does not treat blockchain as a panacea. It is a substrate for audit and coordination; its value depends on careful role design, privacy-preserving patterns (e.g., channels, off-chain

content, selective disclosure), and humane interfaces that keep the participant in view (Benchoufi et al., 2018; Kakarlapudi & Mahmoud, 2021; Underwood, 2016).

The Canadian public health context underscores the need for such careful design. National and provincial systems share responsibilities for surveillance, prevention, and emergency response; researchers frequently partner with hospitals, agencies, and private data custodians; and legal obligations (e.g., privacy law) intersect with ethics policies and institutional review requirements (Government of Canada, 2019b). The COVID-19 pandemic revealed both the promise and fragility of these arrangements: remote data collection surged; clinical and population studies pivoted rapidly; and long-standing bottlenecks in recruitment, re-consent, and oversight became limiting factors for studies that could have continued safely with appropriate digital infrastructure (Asaad et al., 2020; Hensen et al., 2021). A dynamic, governance-aligned consent platform is not a luxury in this setting; it is a precondition for resilient, trustworthy research that can scale and adapt.

## 1.2 Problem Statement

The problem to be addressed by this thesis is the inadequacy of Traditional Informed Consent (TIC) in the current digital age (Barney & Antisdel, 2013; Biros, 2018; Musmade et al., 2013; O'Neill, 2003; Sugarman et al., 2005). Public health researchers want to collect Personal Health Information (PHI) from IoT and Smart devices owned by the general population to conduct studies. However, collecting and maintaining TIC from large cohorts of data subjects is costly since it requires archiving and managing TIC forms, time-consuming because data subjects must be in-person with the researcher to provide Informed Consent (IC), susceptible to human errors due to analog and paper-based management and storage, and likely to suffer from selection bias which consequently makes the research outcome not to represent the general population. Biros describes how, most times, traditional informed consent is treated as a mere document to comply with laws and regulations, and not as an ongoing process, which reiterates the fact that support from digital health technologies is needed to improve data subjects' protection. (Biros, 2018).

The continued use of TIC directly affects how fast and often the general population benefits from the research's outcome. Research's outcome quality, efficacy, and effectiveness are affected by not leveraging more fit-for-purpose and better representative datasets (Helliwell & Massera, 2022; Loftus et al., 2018). Privacy and cybersecurity concerns regarding the inappropriate storage of Personal Identifiable Information (PII) pose risks to data subjects. Paper forms are not always the best way to convey information, sometimes resulting in information overload and inappropriate grant of consent. TIC lacks dynamic features when a researcher changes a study protocol; in-person re-consent is needed from all participants, increasing study length and costs (Barney & Antisdel, 2013; Biros, 2018; Musmade et al., 2013; Sugarman et al., 2005; U.S Food & Drug Administration, 2018). In the work by Biros, (Biros, 2018), the author discusses the importance of the subject's autonomy and the vulnerabilities of TIC, and how important it is to try to mitigate these problems. The author also mentions that alternative ethical methods of obtaining informed consent are necessary to address the limitations of new regulations and participants' values. Another challenge of traditional informed consent is that the communication between the researcher and data subjects is limited to in-person inquiries only in most cases, which limits changes to the study protocol and the ability of data subjects to continuously communicate with researchers during the conduction of the study. In (Ackerman & Proffit, 1995), they were already discussing the limitations of TIC in conveying research's risks, benefits and outcomes to patients, and mentioned how early orthodontic software helped to ensure patient informed consent was sound rather than relying only on patients' interpretation of words on a piece of paper. Participation bias is a consequence of TIC since limited cohort sizes are less statistically powerful. Ethical review boards and other oversight authorities have limited surveillance and rely on reports to supervise study conduct. Finally, third parties representing data stewards who control access to siloed data hesitate to share PHI for research due to the lack of appropriate data governance infrastructure, thus losing opportunities for data-sharing agreements for innovation that are synergic with the goals of public health research.

Hence, overcoming TIC limitations is of significant importance for the future of public health research since it will facilitate new opportunities for research due to the variety and richness of PHI from IoT and smart devices. Moreover, studies would have a better representation of the general population since researchers would not be geographically limited to nearby participants and could recruit much larger cohorts of participants, improving the statistical power of studies. Public health policies and interventions would have robust evidence-based studies, possibly improving precision in estimations. Facilitating longitudinal studies on a national scale would be easier and more cost-effective, and better guide health promotion efforts.

Public health research could benefit from overcoming limitations and challenges imposed on public health research by traditional informed consent limitations, such as high costs and inefficient manual processes. The concept of Dynamic Informed Consent (DIC) is the leading approach to overcome TIC limitations because DIC is the digital representation of TIC. Dynamic informed consent includes all components of TIC and enhances them with modern technologies such as remote communications, remote recruitment, remote auditing of study protocol and consent forms, empowers data subjects to control their study participation, and provides opt-in and opt-out natively. DIC provides transparency tools that improve trust without compromising PII from participants by leveraging modern cybersecurity techniques. However, most DIC solutions are not designed for public health research and are also not developed with Canadian laws and Regulations in mind.

There are data governance frameworks for health data in Canada, such as the CIHI's Health Data and Information Governance and Capability Framework; however, the lack of a specialized data governance framework for modern public health research that could guide researchers in achieving data-sharing agreements more efficiently still needs to be developed.

# 2 Background

This section situates the thesis within the intersecting bodies of literature on public health research, informed consent, data governance, and digital infrastructures. It reviews the conceptual, ethical, and technical foundations necessary to understand why traditional consent models struggle in data-intensive, inter-organizational research environments, and how emerging approaches, such as dynamic informed consent, formal data-governance frameworks, and ledger-based audit mechanisms, have been proposed to address these limitations. Rather than providing an exhaustive review, the background focuses on the constructs and challenges most directly relevant to the design and evaluation of a governance-aligned, participant-centred consent platform for public health research.

## 2.1 Challenges to Data Collection in Public Health Research

Personal Health Information (PHI) is a big enabler of the new era of public health research and intervention; however, it comes with challenges. The technical and strategic challenge of utilizing PHI for public health research is obtaining and maintaining proper informed consent from data subjects. Most public health research currently occurs on top of anonymized datasets void of Personal Identifiable Information (PII), thus, in most cases, not requiring explicit informed consent from data subjects. However, as research on PHI grows in popularity, public health researchers avoid clinical trials and other research modalities that require either probing/intervention of the data subjects over the study life cycle or research that requires Personal Identifiable Information (PII) from data subjects. The main reason for this is the flaws and limitations of the infrastructure used to collect and maintain Traditional Informed Consent (TIC) from a large pool of participants, which can comprise thousands of participants geographically distributed with large distances between researchers and data subjects. Traditional Informed Consent is a process that includes documentation that ensures the protection of data subjects' mental and physical health integrity during the entire research life cycle. In fact, during the COVID-19 pandemic, one of the limiting factors for data collection and execution of clinical trials was the lockdowns and unestablished safety protocols that halted a significant number of clinical trials (Asaad et al., 2020).

It is important to clarify that not all clinical trials and research that were stopped by the pandemic needed to be stopped. A multitude of these studies could have been continued if all the research and clinical trial protocols had the necessary digital infrastructure to connect with data subjects. Cases of changes in research protocols which would require obtaining re-consent from participants could have been done remotely and with the use of digital signatures and certificate authorities. The signed consent forms could have been stored in a secure and private environment. Communication between researchers and data subjects could be done via video calls, with support from digital media, such as video and images, to ensure a proper understanding of the informed consent form. Most data collection could have been provided via digital forms, and data collected via IoT, smart and wearables devices, without needing the data subject to be physically present at a hospital, clinic, or university. Finally, any authority performing audits or requiring study information could obtain such data digitally.

To achieve such a digital research environment, the concept of Dynamic Informed Consent (DIC) (Budin-Ljøsne et al., 2017; Mamo et al., 2020; Scott et al., 2018; Stein & Terry, 2013) is introduced. Dynamic Informed Consent is a digital and portable version of traditional informed consent, meaning that it includes all capabilities of TIC, and enhances them to be remotely adapted, includes automation of consent and re-consent collection, allows for oversight from appropriate authorities, study protocol and DIC form approval pipeline, privacy protection of data subjects, and allows for stakeholders, especially, data stewards to verify consent information before sharing PHI with researchers.

The next two sections will explain the differences between traditional informed consent and DIC and how transitioning to DIC can help to mitigate problems currently faced by researchers, not only during the pandemic but, in the same way, could be beneficial for the future of PHI research in public health.

## 2.2 Challenges of Bigdata Analysis

Most big data analysis relies on infrastructure, methods, and knowledge translation and transfer. The infrastructure needed to work with big data is not trivial and depends on and requires (I) interoperability between different resources and data sources, (II) data collection, (III) data storage, (IV) data processing

and (V) knowledge transfer (Demchenko et al., 2014). More details about each point can be found in Appendix G.

## 2.3 Traditional Informed Consent Form Limitations

As mentioned in the introduction, traditional IC is currently not enough to provide researchers with the means to collect IC from large cohorts of data subjects without having massive costs and logistics challenges. Moreover, a significant portion of public health research is conducted using PD and PHI collected outside a clinical environment (Benchoufi & Ravaud, 2017b; Gómez-Barroso et al., 2018; IBM, 2018; Li et al., 2016), and as such, depends on obtaining IC from data subjects that are distributed over large geographical ranges. Some datasets containing anonymized PD and PHI from a large portion of the population are provided by big-tech companies such as Apple and Google (Google Inc., 2022; Strzelecki, 2022), public health researchers would benefit by being able to directly select the cohort better suited for their research question.

Management of IC is also a relevant challenge to public health researchers due to the large cohorts of data subjects required for public health research over communities, provinces, and national levels. For this reason, most public health research is either executed in small cohorts, which limits the validity of some studies due to not representing a significant portion of the population, or it forces researchers to utilize datasets that are not the most appropriate for their study (Khokhar et al., 2014).

Finally, another limitation of traditional IC is the information overload (Bester et al., 2016; O'Neill, 2003) that the ICF possesses in some cases. The presumption that all data subjects are capable of understanding all the interventions, privacy agreements, risks, benefits and alternative options depends directly on the principal investigator's communication skills to clarify any doubts from data subjects. Even an ICF approved by an IRB can contain topics and terminology that are hard to understand by data subjects with only textual descriptions and very bureaucratic language. With the current digital landscape, most data subjects have access to a smartphone and/or computer that can provide much more friendly visualizations

of the ICF, as well as multiple sources of knowledge transfer that the data subject can utilize to understand the ICF and what they are submitting themselves to when agreeing to an ICF.

## 2.4 Dynamic Informed Consent

Researchers must deal with regulatory, ethical and privacy concerns to obtain and maintain proper informed consent. However, traditional means of consent are not as fast, flexible, scalable, secure and dynamic as the current digital landscape we are living in. To address these problems, the concept of Dynamic Consent (DC) has been proposed as a new way of ensuring that research can adapt to new technologies and regulations (Budin-Ljøsne et al., 2017; Kaye et al., 2015a; Knifed et al., 2008; Scott et al., 2018).

Dynamic consent systems are built on top of distributed systems architectures (Azaria et al., 2016; Chua et al., 2019; ISO, 2019; Oldevik & Berre, 1998) that have as their main objectives the facilitation of obtaining informed consent from data subjects and streamlining communication between data controllers and data subjects. With DC systems, researchers can recruit large-scale participants through virtual informed consent forms that can be accessed by mHealth apps. Changes during research phases that require re-consent can be done by mHealth apps without increasing research costs (Steinsbekk & Solberg, 2011).

Dynamic consent offers several strengths, including enhanced control for data subjects and improved access to personal data for researchers. Its advantages include optimized recruitment processes, leading to cost savings in research; efficient re-consent acquisition in dynamic research settings; regulatory flexibility, ensuring compatibility with various healthcare regulations; empowerment of data subjects through control over their personal data, promoting data sovereignty and autonomy; enhanced engagement opportunities for more meaningful interactions with data subjects; and the advancement of scientific research by creating a dynamic environment for consent management. However, dynamic consent also presents challenges. It needs to address inclusivity for specific demographics, such as the technologically averse or those with accessibility challenges, to prevent digital divides. The volatility of participant pools, with the ease of opting out, poses a risk to research continuity. Additionally, addressing the broader digital

divide is crucial to ensure equitable representation and participation, as those without technological access could be excluded from research endeavours.

## 2.5 Dynamic Informed Consent Management Solutions

Before any researcher begins to implement any study design, he must first have the necessary infrastructure to obtain and maintain Informed Consent (IC) from all data subjects (Budin-Ljøsne et al., 2017; Kaye et al., 2015a; Knifed et al., 2008; Scott et al., 2018). Consent Management refers to the systematic approach of overseeing and documenting the permissions and preferences expressed by individuals concerning the collection, storage, and use of their personal data (Kakarlapudi & Mahmoud, 2021). Traditionally, the process of IC management was paper-based, and the researcher and patients had to be in the same place to ensure proper disclosure and understanding from data subjects. With the recent advances in IoT, big data, and wearables, it is now impractical for researchers interested in a large cohort, RCTs, case-control and other study designs to keep with traditional means of consent for thousands if not millions of participants (Grady et al., 2017).

Dynamic Consent (DC) (Budin-Ljøsne et al., 2017; Scott et al., 2018) is a digital representation of traditional IC management with enhanced capabilities, such as remote communications between data subject and researcher, patient control over enrollment (opt-in and opt-out) and personal data. DC also offers more knowledge transfer resources to ensure proper disclosure and understanding of data subjects. Moreover, DC management is a process, meaning that any changes during the research trigger the need to obtain re-consent from data subjects. A DC platform must be capable of communicating with all participants through digital means (e.g. mHealth apps, emails, push notifications) and obtain re-consent to continue with the study.

## 2.6 Data Governance

Data Governance (DG) dictates the rules, roles, actors, responsibilities, and accountabilities for organizations to ensure that data is properly handled. More specifically, DG's main principles focus on data

quality, data access, data control, data integrity, and data security processes, and the effects and consequences when these principles are violated by the Data Management's (DM) domain. A proper DG framework should guide actors and processes on how to reach appropriate decisions over the data lifecycle. In (Marina Micheli et al., 2020), the authors state that governance refers to the web of actors with different roles involved in the processes of a governing system, and that governing is the result of a process, not only occurring from rule creation and enforcement, but also includes social interactions, cooperation, and negotiation between stakeholders at the horizontal level.

## 2.7 Data Governance Models

Recently, data governance has returned to the forefront of academic research as an imperative for obtaining PHI and PD from data subjects and data stewards. This is mainly due to legal liabilities, regulations, and the varying requirements of each stakeholder involved in the data-sharing process. To establish a Data Sharing Network (DSN) (Kim et al., 2014), requirements from all stakeholders' DG policies and rules must be mapped. The type of relationship that each stakeholder will practice, and what role each one of them will have on the DSN is also necessary to be pre-emptively defined so that data transactions can be integrated into their internal processes. For example, in (Marina Micheli et al., 2020), the authors defined four models of DG for data sharing that came from a literature review and analysis of previous DSNs. Please see Appendix H for details.

## 2.8 Ledger Technologies

Ledger technologies, most notably blockchain, provide a distributed and append-only infrastructure for recording events across a network of peers without reliance on a single central authority. Transactions, such as consent grants, modifications, or withdrawals, are validated through consensus mechanisms and permanently recorded as timestamped entries cryptographically linked to prior records, producing an immutable audit trail (Gorenflo et al., 2019). This structure makes ledger technologies particularly suitable for data-governance contexts where traceability, non-repudiation, and accountability are essential.

In the context of dynamic informed consent, ledger technologies enable consent decisions to be treated as first-class governance artefacts rather than static documents. Each consent action can be recorded as a discrete, verifiable transaction, allowing researchers, data custodians, and auditors to reconstruct the full consent history associated with a dataset or study lifecycle (Gorenflo et al., 2019). This supports regulatory compliance by providing demonstrable evidence of when consent was granted, modified, or revoked, and under which conditions such actions occurred (Marelli & Testa, 2018).

From a privacy and access-control perspective, modern ledger systems rely on public-key cryptography, digital signatures, and role-based authorization to authenticate participants and restrict operations to approved actors (Zyskind et al., 2015). When deployed as permissioned ledgers, access to the network itself is limited to verified institutions, enabling governance rules to be enforced at the infrastructure level while preserving decentralization among trusted parties (Kuo et al., 2017). Rather than storing raw personal health information on-chain, ledgers are typically used to record hashes, pointers, or policy states, thereby supporting auditability without unnecessary data exposure (Marelli & Testa, 2018).

Overall, ledger technologies function as governance substrates that complement, rather than replace, existing legal and ethical frameworks. Their primary contribution lies in enforcing procedural integrity, ensuring that data access and use remain continuously aligned with dynamically expressed consent and formally defined governance rules, while producing an auditable, tamper-evident record suitable for oversight and accountability in public-health research environments (Gorenflo et al., 2019; Kuo et al., 2017; Underwood, 2016).

### 2.8.1 Private Ledger

A private and permissioned blockchain can accept transactions from registered users only. It also does not allow for the information of the transactions to be read by anyone (Chua et al., 2019; Guegan, 2017; Jones et al., 2019). A private blockchain works under a consortium network in which members (peers) transact information privately. Communications between members are done through communication channels that can hold only a subset of members. This allows for private parallel communications between members of

the consortium, reducing the incidence of internal breaches of privacy. Another advantage of a private blockchain is that data subjects do not directly interact with the blockchain layer by keeping wallets with keys and credentials (Zheng et al., 2018). All interactions are done through a web interface that one or multiple members of the network host. This reduces the requirements and complexities for conducting research that uses DC and reduces the risks of data subjects losing keys and not accessing their data anymore.

Data control for data subjects can also be optimized by private blockchain networks. For example, any stakeholder who wishes to process personal data must register via the DC platform, formally create a DC form, deploy it to an IRB, and begin recruiting data subjects from the platform. Since all data controllers and processors are members of the network, each time a data subject grants or revokes consent to a study, all members are automatically notified of this change and must act accordingly. In the case of some data processors or third parties not respecting the revocation of consent, the platform can provide the history of consent for the data subject as auditable information for their protection (Zheng et al., 2017a).

### 2.8.2 Ledger Governance

The governance model of the ledger network's decision-making utilizes guidelines and requirements derived from the generated data governance model, which will be presented in the next sections.

#### 2.8.2.1 The Hyperledger Fabric Ledger

The Hyperledger Fabric (HF) (Hyperledger Foundation, 2026a) platform is an open-source, permissioned, distributed ledger technology (DLT) platform (Androulaki et al., 2018a; HyperledgerDocs, 2018) developed to be used under enterprise contexts. All enterprise interactions are performed in a private network environment called Hyperledger Fabric Network (HFN). An HFN provides blockchain services so that client applications and network administrators can interact with the HFN proposing new transactions and querying the blockchain. In a HFNs context, a consortium (Hyperledger Foundation, 2026b) is comprised of two or more organizations on the HFN that need to transact business with each other.

In Hyperledger Fabric, an Organization (Github, 2019) is a logically driven group of members that can represent big or small corporations. Each HFN organization is composed of members called Peers (Hyperledger, 2019a). Peers are responsible for hosting ledgers, smart contracts, handling changes to the ledger, communications between different organizations (channels), and managing external requests from applications. An Endorsing Peer is responsible for executing smart contracts over a transaction thesis from a client to verify its validity before it can be added to the ledger. A Committing Peer is a member who keeps a copy of the ledger without any smart contracts, meaning that this is done to keep multiple copies of the ledger to avoid single-point failures. Ordering peers and organizations (Hyperledger, 2019b) are responsible for keeping the communication sound between the participants of a channel. More details about Hyperledger fabric can be found in Appendix A.

## 2.9 Challenges of Big Data Collection for Public Health Research

The Public Health Agency in Canada is responsible for promoting health, preventing and controlling infectious diseases and injuries, preventing and controlling chronic diseases and injuries, knowledge transfers between Canada and the rest of the world, preparing and responding to public health emergencies, research and development of Canada's public health programs, and to strengthen international collaboration on public health and coordinate national strategies to public health and planning (Government of Canada, 2019a). Recently, due to the advances in big data and IoT technologies public health agencies have possible access to large amounts of data generated from smart devices (e.g., smartphones, smartwatches), wearables (e.g., fitness bands, smart clothing), and environmental sensors (e.g., smart thermostats, air pollution sensors)(Bagot et al., 2018; Firouzi et al., 2018; Zheng et al., 2017b).

Big data in public health generally originated from Electronic Health Records (EHR), Personal Health Records (PHI), Medical Practice Management Software (MPM), healthcare provider data, genomics data, and data collected from IoT devices. Mainly, EHR, PHI and IoT data are often the most common and present in public health research. EHR is data collected from hospitals and clinics, and normally is generated from vital signs monitors, medical reports, and Hospital Information Systems (HIS). PHI is data generated

from personal smart devices, wearables and sensors owned by people (Data Generators or Data Producers). Finally, IoT data is data collected from IoT devices connected to the internet, continuously generating data streams.

Big data has been applied in public health to help with better identification, monitoring, assessment, prevention, and treatment of diseases, it is also used for generating insights to help the creation of better public health interventions. For example, big data can provide national or global-scale information about smoking, drinking, drugs, exercise, chronic health conditions and mental health, which, when provided to public health researchers, can provide invaluable behavioural information on large scales that were not possible before big data was widely available (Ajunwa et al., 2016; Balan et al., 2017; Barrett et al., 2013; Chen et al., 2017; Gamache et al., 2018; Kramer et al., 2014; Martin-Sanchez et al., 2017). Big data also provides public health means to accelerate the timing from acquiring knowledge to translation and transferring knowledge to the proper target audience (Khoury & Ioannidis, 2014).

# 3 Motivation

The following few sections will discuss the motivation of this work, which in summary is to bring informed consent process to the digital era, empowers data subject data control, facilitate consent collections for public health researcher, and demonstrate how newer technologies, such as blockchain(Grishin et al., 2018; Guegan, 2017; Lo et al., 2019; Velmovitsky et al., 2020; Xie et al., 2018; Zheng et al., 2018) can be used in this scenario to improve trust.

## 3.1 From Medical Oaths to Formal Codes

**Ancient and early medicine:** The earliest recorded precursor to informed consent is the Hippocratic Oath (c. 400 BCE). This oath, attributed to Hippocrates, instructed physicians to care for patients, avoid causing harm (the maxim "*primum non nocere*"), [1]and respect confidentiality (Kerpel-Fronius et al., 2018). The principles of beneficence, non-maleficence and confidentiality served as a moral compass for medieval and early Islamic physicians. Abu Ali al-Hussein Ibn Sina (Avicenna), writing The Canon of Medicine in the eleventh century, synthesized Greek and Arabic medical knowledge and insisted on observing patient welfare and informed treatment, preserving the ethical tradition throughout the Middle Ages.

**Early modern innovations and emerging ethics**: In the eighteenth century, scientific advances accelerated. Edward Jenner's pioneering smallpox experiments in 1796 involved inoculating an eight-year-old boy with cowpox material and subsequently exposing him to smallpox; when the boy did not contract smallpox, Jenner concluded that cowpox could provide immunity (Kerpel-Fronius et al., 2018). Jenner's Inquiry into the Causes and Effects of the Variolae Vaccinae described sixteen cases demonstrating that cowpox produced only mild illness yet protected against smallpox (Kerpel-Fronius et al., 2018). This marked the beginning of vaccinology and introduced the notion that individuals could consent to preventive interventions for their own benefit and the good of society. In the early nineteenth century, René Laënnec invented the stethoscope (1816), revolutionizing diagnostics, and Thomas Percival's Medical Ethics (1803)

[1] This maxim is associated with the Hippocratic Oath. However, the English physician Thomas Sydenham is believed to have composed this Latin phrase (Bernstein, 2022; Smith, 2005).

codified professional duties toward patients, emphasizing honesty and patient welfare. While these innovations were ethically progressive, research participants were still largely passive recipients of physician decisions.

**Birth of clinical trials:** One of the first controlled clinical experiments took place in 1747 when James Lind treated sailors suffering from scurvy with different dietary interventions. His trial identified citrus fruit as an effective treatment, demonstrating the value of systematic experimentation. However, trial participants were not fully informed and had little autonomy over their participation. By the mid-nineteenth century, germ theory emerged through the work of Louis Pasteur and Robert Koch. Pasteur's experiments demonstrated that microorganisms cause infection and led to pasteurization techniques; he emphasized laboratory control and reproducibility (Kerpel-Fronius et al., 2018). These advances shaped modern public health but relied on observational studies without explicit consent protocols. Florence Nightingale's work during the Crimean War (1850s) introduced nursing as a profession, improved sanitation and highlighted patient dignity. Yet, paternalistic attitudes persisted, as exemplified by J. Marion Sims' gynecological experiments on enslaved women in the 1840s, which were performed without anesthesia or consent.

## 3.2 Twentieth-Century Ethical Milestones

**Early abuses and the first codification**: Biomedical progress continued into the twentieth century with the discovery of penicillin (1928). At the same time, unethical research practices became increasingly visible. The U.S. Public Health Service's Untreated Syphilis Study at Tuskegee (1932-1972) followed 399 Black men with syphilis and 201 control participants, but did not obtain informed consent and withheld treatment even after penicillin became available (Brandt, 1978). The study ended only after public exposés in 1972; it prompted sweeping changes to research regulation and emphasized the need for voluntary consent.

**International responses**: After revelations of Nazi atrocities, the 1947 Nuremberg Code established ten principles for ethical research. It defined voluntary consent as "essential" for human experimentation, requiring that participants be legally competent and free from coercion (Hiroyuki Nagai et al., 2022). The

Nuremberg Code also insisted that experiments should yield fruitful results for society and avoid unnecessary suffering. These principles inspired the World Medical Association's Declaration of Helsinki in 1964, which charged physicians involved in research to protect the life, health, dignity, autonomy and confidentiality of human subjects (Kerpel-Fronius et al., 2018). By 1979, the U.S. National Commission's Belmont Report codified three overarching ethical principles: respect for persons, beneficence and justice and their application to informed consent, risk–benefit assessment and equitable subject selection. Together, these documents laid the foundation for formal ethical oversight, institutional review boards and participant protections.

### 3.3 Contemporary Challenges And Innovations

**Genetic research and privacy:** Advances in genomics intensified ethical debates. The 1990–2003 Human Genome Project raised concerns about genetic privacy, potential discrimination and the use of biological samples beyond the original consent. In response, the U.S. Health Insurance Portability and Accountability Act (HIPAA, 1996) introduced legal protections for patient information. High-profile data misuse incidents, such as the 2018 Facebook–Cambridge Analytica scandal and the 2020 COVID-19 pandemic, exposed the fragility of traditional consent. Emergency use of data and vaccines highlighted tensions between public health and individual autonomy. Additionally, the discovery of racial bias in clinical algorithms revealed that modern health technologies can perpetuate inequities. A 2019 Science study showed that a widely used risk-prediction algorithm assigned lower risk scores to Black patients, meaning they were far sicker than White patients at the same score (Obermeyer et al., 2019). The bias arose because the algorithm predicted health-care costs rather than illness, and due to unequal access to care (Obermeyer et al., 2019).

**Dynamic informed consent and participant empowerment**: Traditional informed consent one-off agreement at enrolment struggles to accommodate new data uses, large-scale biobanking and digital health research. Dynamic consent emerged in the 2010s as a participant-centric approach. It is an interactive, personalized platform that enables participants to engage in research as much or as little as they prefer and to amend their consent decisions in real time (Prinsen, 2024). Dynamic consent centralizes transactions and

communications and allows participants to give or withdraw consent for specific uses, thereby keeping an ongoing record of their decisions (Prinsen, 2024). Such systems allow preferences to be tailored, enable re-contact and provide fine-grained control over data use (Prinsen, 2024). Participants can modify consent as circumstances change, which improves autonomy and trust (Prinsen, 2024). Dynamic informed consent aims to foster transparency and reciprocity: the platform serves as a communication forum where researchers provide feedback and participants remain informed (Prinsen, 2024). It thus addresses major limitations of traditional consent by promoting continuous engagement and respecting participant choices.

**Blockchain-based audit trails**: Recent proposals combine dynamic consent with private ledger technologies to create immutable audit trails and automate consent enforcement. Blockchain's time-stamping and smart-contract capabilities can create secure, tamper-evident records of consent transactions, improving accountability and data integrity. These technologies aim to prevent the reuse of data without explicit permission and reduce trust asymmetries between participants and researchers.

### 3.4 Chronic Patterns of Unethical Research

Ethical violations have repeated across eras despite evolving guidelines. To illustrate continuity between past and present challenges, Tables 2 and 3 summarize representative cases compiled by (Jones et al., 2016) and modern analogues. Beecher exposed unethical experiments in the mid-twentieth century, revealing that patients were given placebos or injected with cancer cells without being informed, children were deliberately infected with hepatitis, and vulnerable psychiatric patients were involved in research without appropriate consent. Modern data-driven research has produced parallel controversies, including social media mood manipulation, misleading accuracy claims by biotech companies, emergency use of personal data during pandemics and algorithmic discrimination. Table 1 presents a summary of the events and impacts discussed in this section.

*Table 1 - Brief history of informed consent.*

| Date | Historic Event & Description | Impact |
|---|---|---|
| **Ancient medicine (c. 400 BCE)** | **Hippocratic Oath** – A medical ethical framework that emphasized beneficence, non-maleficence (*primum non nocere*), and patient confidentiality. | Foundation for professional conduct; laid the groundwork for later ethical principles. |
| **Middle Ages (500–1500 CE)** | **Avicenna (980–1037 AD)** – Wrote *The Canon of Medicine*, preserving and expanding Galenic and Islamic medical knowledge; emphasized clinical observation and patient care. | Maintained continuity of ethical practice during periods of limited scientific progress. |
| **Enlightenment & early modern medicine (1500–1800 CE)** | **James Lind (1747)** – Conducted one of the first controlled clinical trials aboard HMS *Salisbury* to test scurvy treatments. | Demonstrated the value of systematic experimentation but lacked informed consent. |
| | **Edward Jenner (1796)** – Conducted experiments inoculating a boy with cowpox to demonstrate immunity to smallpox; published sixteen case histories. | Led to the first vaccine and ushered in vaccination as a preventive strategy. |
| | **Thomas Percival's *Medical Ethics* (1803)** – Codified professional duties and patient welfare, influencing later codes of conduct. | Provided an early ethical framework but did not address participant autonomy explicitly. |
| | **René Laënnec (1816)** – Invented the stethoscope, transforming diagnostics. | Improved non-invasive examination and patient care; ethics remained paternalistic. |
| **19th century & rise of medical science (1800–1900 CE)** | **Louis Pasteur & Robert Koch (1850s–1860s)** – Demonstrated germ theory; developed pasteurization; established Koch's postulates. | Revolutionized understanding of infectious disease, enabling modern public health. |
| | **Florence Nightingale (1850s)** – Improved sanitation and nursing practices during the Crimean War. | Professionalized nursing and highlighted the importance of hygiene and patient dignity. |
| | **J. Marion Sims (1840s)** – Performed gynecological surgeries on enslaved women without anesthesia or consent. | Early example of research exploitation and disregard for autonomy. |
| **Early 20th century ethical challenges (1900–1950 CE)** | **Penicillin discovery (1928)** – Fleming's discovery revolutionized infection treatment. | Biomedical breakthroughs continued without comprehensive consent frameworks. |
| | **Tuskegee Syphilis Study (1932–1972)** – U.S. Public Health Service observed Black men with syphilis without obtaining consent or offering treatment even after penicillin became available. | Unethical study highlighted racial inequities and led to reforms in research ethics. |
| **Post-World War II reforms (1950–2000 CE)** | **Nuremberg Code (1947)** – Established voluntary consent as essential for human experimentation. | Landmark code emphasizing autonomy and the necessity of voluntary participation. |
| | **Declaration of Helsinki (1964)** – Instructed physicians to protect the life, health, dignity and autonomy of research subjects. | Provided international standards for research ethics and influenced subsequent guidelines. |
| | **Belmont Report (1979)** – Articulated three ethical principles respect for persons, beneficence and justice and their application to informed consent, risk–benefit assessment and subject selection. | Formed the basis for U.S. regulations and Institutional Review Boards (IRBs). |
| **21st century ethical challenges (2000 CE–present)** | **HIPAA (1996)** – Introduced legal protections for patient health information privacy. | Required new safeguards for data handling; still relies on traditional consent forms. |
| | **Human Genome Project (1990–2003)** – Raised concerns about genetic privacy and secondary use of samples. | Demonstrated need for consent models that accommodate future research. |
| | **Facebook–Cambridge Analytica (2018)** – Exposed misuse of personal data harvested without informed consent. | Highlighted privacy vulnerabilities in the digital age and the inadequacy of broad consent. |
| | **COVID-19 pandemic (2020)** – Emergency use of vaccines and contact-tracing data raised questions about balancing public health with individual autonomy. | Showed that broad consent often fails to cover emergent uses; underscored the need for dynamic consent. |
| | **AI bias in healthcare (2019)** – A study revealed that a widely used risk-prediction algorithm underestimated sickness among Black patients and thus denied resources to those most in need. | Demonstrated how modern technologies can perpetuate inequities and require ethical oversight. |

## 3.5 Beecher's 1966 Exposé and the Continued Violations of Informed Consent in the Modern Era

Beecher's 1966 exposé (Jones et al., 2016) catalogued instances where researchers knowingly violated ethical norms by withholding information from participants, exposing them to harm or exploiting vulnerable groups. These violations occurred despite the existence of professional oaths and early research ethics codes. Table 2 highlights that paternalistic attitudes allowed researchers to ignore autonomy, whether by administering placebos without consent or infecting children and psychiatric patients under the guise of scientific progress. Such cases eroded public trust and spurred the development of modern research ethics.

Table 3 presents the results of a rapid contemporaneous review of informed consent violations that demonstrates that similar patterns persist in the digital age. Social media mood manipulation, misleading diagnostic technologies, emergency data use during pandemics and algorithmic discrimination all illustrate how rapid technological advances can outpace ethical safeguards. The continued exploitation of vulnerable populations and the use of data without informed consent reflect structural inequalities and underscore the need for consent models that are adaptive, transparent and participant-centred.

The history of informed consent reveals an ongoing struggle to balance scientific progress with respect for autonomy and justice. From the Hippocratic Oath's injunction to "do no harm" (Kerpel-Fronius et al., 2018) to the Belmont Report's triad of respect for persons, beneficence and justice, ethical codes have evolved in response to abuses. Yet, as the Tuskegee study shows (Brandt, 1978), regulations alone cannot prevent violations. The digital era introduces new challenges: data can be repurposed indefinitely, algorithms can perpetuate bias (Obermeyer et al., 2019), and crises like pandemics compel rapid action. Dynamic informed consent, aided by data governance and blockchain audit capabilities, offers a path forward by granting participants ongoing control over their data and enabling researchers to maintain transparent, adaptable consent processes (Prinsen, 2024). However, implementing such systems requires addressing disparities in digital literacy, ensuring accessibility for underserved populations and maintaining rigorous ethical and governance oversight. The persistence of consent violations underscores the urgency

of updating traditional informed consent frameworks to protect participants in an era of ubiquitous data and advanced technologies.

*Table 2 - Beecher's examples of informed consent violations (1966).*

| Type of informed consent violation | Beecher's examples (1966) | Reference |
|---|---|---|
| **Placebo without consent** | Patients were administered placebos without being informed, violating their right to autonomy. | Beecher H.K. (1966). *Ethics and Clinical Research. The New England Journal of Medicine*, 274(24), 1354–1360. |
| **Injected cancer cells** | Elderly and chronically ill patients were injected with live cancer cells without proper disclosure. | Beecher (1966). |
| **Willow brook Hepatitis Study** | Children at the Willow Brook State School were intentionally infected with hepatitis without appropriate informed consent. | Beecher (1966). |
| **Mentally ill patients in research** | Vulnerable mentally ill patients were subjected to experiments without appropriate consent. | Beecher (1966). |

*Table 3 - Modern examples of informed consent violations.*

| Type of informed consent violation | Description | Modern examples | Reference |
|---|---|---|---|
| **Placebo without consent** | Participants were not told they were receiving an inactive intervention. | Facebook Emotional Contagion Study (2012): manipulated user emotions without informed consent. | *(Robinson Meyer, 2014)*. |
| **Injected cancer cells/biological material without disclosure** | Live cells or tissues are injected without proper informed consent. | Theranos scandal (2015–2018): patients were misled about the accuracy of blood tests. | (Randazzo & Sommerville, 2021). |
| **Deliberate infection without consent** | Exposing participants to pathogens without clear consent. | COVID-19 data usage: debates over emergency data collection without clear consent protocols. | (Hensen et al., 2021). |
| **Research on vulnerable populations without consent** | Experiments conducted on vulnerable groups without proper consent. | AI bias in healthcare algorithms: a widely used risk-prediction algorithm exhibited racial bias against Black patients[7]. | (Obermeyer et al., 2019). |

As argued in the previous sections, the main motivation for this work is to overcome the challenges and limitations that public health researchers face when conducting studies that use PD and PHI from the general population by providing a platform that facilitates the collection and maintenance of informed consent. Through the developed platform, public health researchers gained the ability to collect IC from large cohorts of data subjects at low cost and with enhanced capabilities they did not possess before.

A secondary motivation was the development of a data governance model for public health research over PHI and PD to help guide stakeholders interested in this field. The data governance model defines the

actors, social norms, nodal points, roles, and requirements for public health research over the PD and PHI ecosystem. The framework was used as requirements for developing the platform and plays a vital role in data governance by providing a trusted environment in which data subjects and researchers can provide and collect IC, and, at the same time, facilitating interactions and decision-making between researchers, data custodians, and data auditors.

# 4 Work Completed

This thesis pursued three aims that together articulate and test a governance-to-platform path. First, it developed an inter-organizational data governance framework tailored to public health research that combines the GAF's analytical discipline with the PDS orientation toward participant agency. The framework specifies actors, nodal points, norms, and transaction types, and it aligns them with concrete duties, approval gates, revocation propagation, and audit obligations so they can be implemented rather than merely described (Aeberhard & Rist, 2011; Pedro & Morita, 2022; Velmovitsky et al., 2020). Second, it implements those duties in Consentio, a modular, dynamic consent platform whose architecture separates participant-facing disclosure and control from back-office orchestration and ledgered audit, using Hyperledger Fabric to maintain a permissioned consent history endorsed by relevant organizations (Androulaki et al., 2018a; HyperledgerDocs, 2018). Third, it evaluates the platform with target users using validated instruments for usability and skills alongside thematic analysis of open-ended feedback, with special attention to transparency, trust, and the practical intelligibility of consent history and re-consent prompts (Braun & Clarke, 2006; Cassidy & Eachus, 2002; Lewis, 2011; Murphy et al., 1989; van Deursen et al., 2015; Will, 2026).

Two additional clarifications are important for readers who are encountering consent debates for the first time. The first concerns scope. This thesis does not argue that consent alone is sufficient to address all ethical challenges in data-intensive public health. Consent is a necessary condition for respecting persons, but justice and non-maleficence require scrutiny of sampling, measurement, modelling, and deployment, e.g., ensuring that risk prediction does not divert resources away from those with greatest need. (Obermeyer et al., 2019). The second concerns accessibility. Because consent must be meaningful for diverse publics, platforms that purport to "empower participants" but impose heavy cognitive or technological burdens risk reproducing inequities. Accordingly, the platform emphasizes layered disclosure, plain-language summaries, and participant controls for revisiting decisions, and the evaluation

attends to digital literacy and perceived information quality. (Bester et al., 2016; Budin-Ljøsne et al., 2017; Prinsen, 2024).

This thesis undertakes a comprehensive program of work to modernize informed consent management for public health research. The research progresses through four major undertakings:

- **Development of an IODG framework (Section 6):** Building on the Governance Analytical Framework, the thesis maps the ecosystem of public health research, its actors, decision rights, social norms and transaction types, and derives an Inter Organizational Data Governance model. The model emphasizes personal data sovereignty, allocates responsibilities to researchers, data custodians, regulators and data subjects, and outlines phased implementation and auditing mechanisms.
- **Translation of governance into a dynamic consent platform (Section 7)**: Governance requirements were decomposed into concrete system specifications. Use case and class diagrams defined entities and actor capabilities, state diagrams and formal logic expressed legal lifecycles and invariants, and an Angular implementation enforced these rules. A private ledger component provides tamper-evident records, ensuring that every consent or data sharing event is auditable.

**Quantitative user experience evaluation (Section 8):** Ten participants (researchers and data subjects) interacted with the Consentio prototype and completed standardized surveys. Measures included the Post Study System Usability Questionnaire (PSSUQ), Internet Skills Scale (ISS), Computer User Self-efficacy (CUSE), a customer satisfaction questionnaire and a Net Promoter Score (NPS). Results showed high usability (global PSSUQ mean = 1.82), moderate to high digital skills (ISS mean ≈ 3.75/5), moderate self-efficacy (CUSE mean ≈ 2.96/6) and positive NPS scores.

**Qualitative reflexive thematic analysis (Section 9):** Semi-structured interviews and open-ended survey responses from participants and researchers were analysed to understand nuanced perceptions. Themes uncovered included the desire for clear revocation limits, the importance of explaining ledger security, tensions between efficiency and informedness, motivation through centralized dashboards and

feedback, and researchers' needs for customization and enhanced notification features. This analysis led to design recommendations and highlighted tensions between autonomy and practicality.

These phases collectively demonstrate how a principled governance framework can be translated into a functioning, auditable dynamic consent system and evaluated from multiple stakeholder perspectives.

# 5 Thesis Organization

This thesis is organized as follows. Section 6: The development of a data governance framework for public health. Section 7 describes the development and deployment of a blockchain-based Dynamic Consent platform leveraging the principles developed in Section 6. Section 8 presents the methods, application, and results of the quantitative user experience surveys applied before and after users utilized the platform. Section 9 presents the methods, application, and results of the thematic analysis synthesis of the interviews with participants, a discussion that includes its findings and limitations, and an overall reflection on the results mapped against each preceding section to evaluate their relevance. Finally, Sections 10, 11, 12, and 13 present the thesis summary of design implications, limitations, contributions and conclusion.

# 6 An Inter-Organizational Personal Data Sovereignty Governance Framework for Public Health Research

## 6.1 Introduction

Data Governance (DG) has been used in the corporate domain since its inception in the 1990s and 2000s (Abraham et al., 2019; CIO Central Guest, 2017; Evren et al., 2021; Nielsen, 2017). Most large-scale and multinational companies have a DG program and committee, although with varying maturity levels, that describe the company's data strategy, policies, guidelines, and decision-making rights (Al-Badi et al., 2018; Alhassan et al., 2019; Cheng et al., 2018; Kim & Cho, 2018; Li et al., 2019; Panian, 2010). The rise of DG as a topic for research and implementation by academia and industry, respectively, is due in part to the advances of IoT, smart devices, home sensors, and cloud-based systems. These technological advances allow companies and researchers to gain access to massive datasets with value for industry and research.

Industry's DG objectives are to provide guidelines for managing, securing, and utilizing the data of the company and its users, whilst maintaining alignment with the company's data strategy(Calder, 2019; Gregory, 2011a; Thomas, 2010). However, although public health (PB) researchers' DG objectives align with industry's DG objectives, additional goals inherited from public health research principles (Anomaly, 2011; Horton et al., 2014; Lopez, 2010; Mowat & Butler-Jones, 2007; Schröder-Bäck et al., 2014), which aim to monitor and improve population health, and improve public health interventions and policies quality. These "extra" DG objectives add complexity to the work of public health researchers (Anomaly, 2011; Benke & Benke, 2018; Gamache et al., 2018; Khoury & Ioannidis, 2014; Walport & Brest, 2011), since to obtain datasets containing the general population's PD, public health researchers must comply with acts and laws regulating biomedical research over PD, as well as DG requirements that industry partners demand in order to share PD datasets with researchers (Katal et al., 2013; Rothwell et al., 2021; Tse et al., 2018a).

## 6.2 Public Health Research Access to Personal Health Information

Traditionally, public health researchers collected Electronic Medical Records (EMR) on their own premises with their own medical devices and observations. The collected EMR data was stored in the organization's own infrastructure, often in paper form. Research objectives and data processing were only negotiated between researchers and Institutional Review Boards (IRBs), with no negotiation between researchers and data subjects beyond collecting informed consent. This is done with an Informed Consent Form (ICF), which presents pertinent information about the study for the data subject's acceptance or rejection.

With the advance of IoT and smart devices (big data), public health researchers desire to benefit from Personal Health Information (PHI) generated from these devices to improve the quality of their research and to explore new research opportunities that were not possible before (Banerjee et al., 2018; Benke & Benke, 2018; Gamache et al., 2018; Graña Possamai et al., 2020; Khoury & Ioannidis, 2014; Laplante & Laplante, 2016; Roski et al., 2017). In this section, we define PHI as a private dataset of personal health information that contains clinical and non-clinical health-related data and information that is owned, managed, and controlled by private citizens. PHI is continuously generated and stored in ad-hoc cloud structures with different guiding principles, social norms, governance frameworks and maturity levels. Hence, accessing such data directly is not possible without a Data Sharing Agreement (DSA) between stakeholders (Fadrique, 2019; Holmes et al., 2014; Kim et al., 2014; Litton, 2017; Phillips, 2018; Walport & Brest, 2011; Wu et al., 2021). Public health researchers must either work with anonymized, pre-made datasets that might not be ideal for their studies, or they need to be capable of complying with stakeholders' data governance requirements in order to negotiate DSAs with multiple stakeholders. However, public health researchers and institutes still lack specific IT and data governance knowledge and the maturity needed to partake in DSA with multiple stakeholders and actors in an inter-organizational data governance environment (Cheng et al., 2018; Holmes et al., 2014; Tse et al., 2018b; Winter & Davidson, 2019a).

## 6.3 Objectives

This section main objective is to provide to public health researchers and stakeholders with a conceptual inter-organizational data governance (IODG) framework for public health research that focus on empowering data subjects (e.g., private citizens) and allow them to have access control of their PHI whilst facilitating researchers' access to PHI and providing data custodians and data owners with the DG mechanisms that the public health domain lacks. The framework presented in this section is meant to be used as a guiding template and discussion piece that must be extended based on each use case. The framework has also considered the guiding principles of public health research in its components to ensure appropriate conduct of biomedical research. Finally, a discussion regarding the framework is presented.

The conceptual framework defines components that are needed to implement data governance in an inter-organizational public health research project. The framework also defines generic entities that should compose those components to ensure that governance requirements and public health research principles are aligned and in synergy. Transactions between these entities are also defined and classified based on the Governance Analytical Framework (GAF) (Aeberhard & Rist, 2011; Hufty, 2008) methodology to expose power imbalances between stakeholders and facilitate preparation for negotiation strategies. Finally, the framework also takes in consideration the General Data Protection Regulation (GDPR), especially article 7 and recitals 33,34,42,43, in which data subjects have control over how their own data is processed and the conditions when informed consent is necessary, public health research principles (European Parliament and Council of the European Union, 2016f; L Marelli, 2018; Phillips, 2018).

We also provide a conceptual model that was created with the objective of showcasing a possible implementation of the DG framework. The use case utilized to build the model was a generic public health research scenario wherein a researcher desires to conduct a study with PHI in an academic setting. The model, described in section 6.10, maps what the actors and stakeholders are, where DG mechanisms should be implemented, what should be monitored, where the nodal points of negotiations are, what DG

requirements need to be defined, what each stakeholder's roles and responsibilities are, and where decision-making rights should be defined.

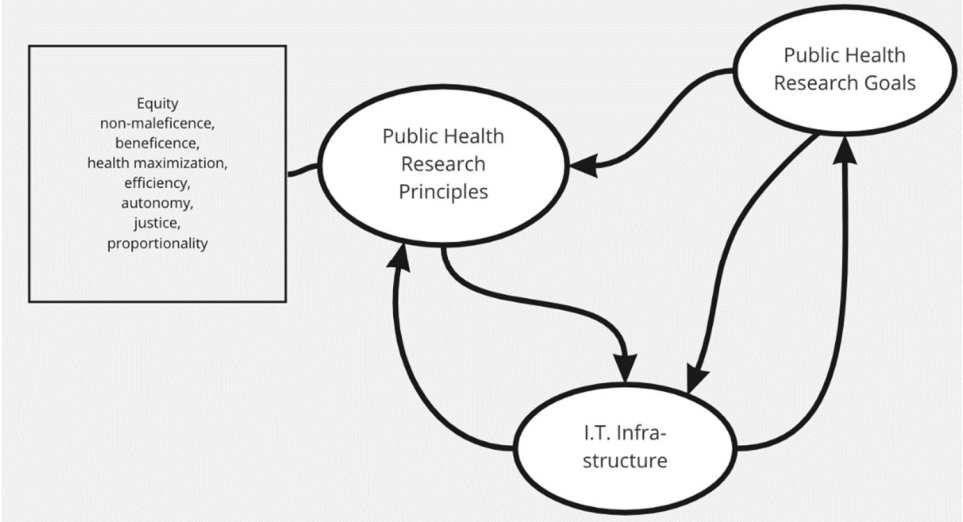
## 6.4 Background

Data governance (DG) is the practice of defining and maintaining the needed processes and strategies for a company's data strategy. Data governance treats data as a business object, thus defining decision-rights and accountabilities over data usage, alongside defining data policies, data standards, and data processes needed to protect and manage data throughout the entire organization. Therefore, data custodians who follow ad-hoc governance guidelines and processes require that research partners that wish to leverage their users' PHI have the same or similar level of DG maturity, which is often not possible. (Gregory, 2011b; Thomas, 2010)

As mentioned in section I, the need for data governance in public health research environments has been steadily growing in recent decades. The term "data governance" first appeared in the literature in the 2000s, after "Data Stewardship" appeared a decade before (Prukalpa, 2021). Data governance gained traction and peaked in 2019 during the rise of the COVID-19 pandemic. The COVID-19 pandemic forced society to engage in social and business activities remotely whenever possible (Asaad et al., 2020; C. J. Wang et al., 2020). The impact of social distancing, prohibition of large gatherings, travel bans, and safety protocols impacted the conduction of traditional public health research as they were not appropriate for the situation (Asaad et al., 2020). Since most of the public health research field is increasingly dependent on PHI, there is a need for more efficient and effective collaboration between all actors involved in research efforts (Tse et al., 2018b). However, the public health domain, including the healthcare domain, lacks maturity in terms of data governance implementation and adoption. This has resulted in inappropriate levels of governance, either excessive or insufficient (John, 2018; McMahon et al., 2019; Tse et al., 2018a). Therefore, our work intends to also present a governance model that aims to help the public health research domain by defining roles, responsibilities, and transactions that each actor and stakeholder should comply with to facilitate researchers' access to PHI.

Furthermore, this work aims to outline how data governance could align with the principles of public health research: equity, non-maleficence, beneficence, health maximization, efficiency, autonomy, justice, and proportionality (Schröder-Bäck et al., 2014). In any modern research, IT infrastructure is critical, from personal devices to large international public health databases. As a component of research, IT must then be aligned with both public health research principles, and the public health research goals that are informed by these principles. At the same time, examining data governance and IT infrastructure brings with it new implications and research directions for public health. With a data governance model specific to the public health research context, there is better support for how these three elements relate to each other and, therefore, what expectations should exist for IT infrastructure. Figure 1 reflects this explanation, modelling the scenarios described above. In this diagram, the edges between public health research goals and IT infrastructure are most relevant to this section, as these are where a data governance framework is needed.

*Figure 1 - Relationship between public health research principles and goals and IT infrastructure.*




In (Abraham et al., 2019), data governance is defined as the exercise of authority over the management of data. It is data governance's goal to implement a corporate-wide data agenda, which maximizes the value of data assets in an organization, and manages data-related risk, such as cybersecurity. Few works on data governance frameworks specific to Inter-Organizational Data Governance (IODG) are available in the literature, tailored specifically for the healthcare and public health domain (Tse et al., 2018a; Winter & Davidson, 2019a). A literature review by (Abraham et al., 2019) provided a conceptual framework that mapped the core principles of data governance found in available literature. Their contributions included the inclusion of a well-established model to illustrate the relationship between governance's antecedents, scopes, mechanisms, and consequences, along with areas where research is still needed. One of the areas identified in their review was regarding governance mechanisms to determine ownership of data, since with that role comes accountability for inappropriate data handling.

Relevance and the need for an effective data governance program are also being embedded into newer regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). More specifically, on GDPR, it thus distributes accountability between the data owner, the data steward, and the data processors. Another gap mentioned in (Abraham et al., 2019), regarding DG research, is the allocation of decision-making authorities, especially under an inter-

organizational environment which involves DSA between multiple stakeholders (Andersen et al., 2014; Broek & Veenstra, 2015; Holmes et al., 2014; Kim et al., 2014). Discussion exists around which is the better approach to allocation of decision-making: decentralized, centralized, or hybrid. Centralized approaches create power imbalances, are less flexible, and incur higher accountability for fewer stakeholders, whilst decentralized approaches require DSA agreements between multiple organizations, which is more difficult to achieve. In IODG environments, not much is known regarding how each organization ensures data ownership and control since each organization has its own DG infrastructure. This lack of DG transparency raises trust issues between stakeholders and creates barriers for IODG, since storage and protection of sensitive data is always a concern in our current digital landscape. Finally, multiple publications mention the need for IODG frameworks to be extensible, meaning that new organizations and policies can be added over time, improving the IODG network quality and increasing its complexity (Abraham et al., 2019; Aisyah & Ruldeviyani, 2019; Al-Badi et al., 2018; Canadian Institute for Health Information, 2020; Kim & Cho, 2018; Li et al., 2019; Thomas, 2010).

Although GDPR provides a useful vocabulary for transparency, access, erasure, and accountability, Canadian public-health research is governed through a different combination of federal privacy law, provincial health-information statutes, research-ethics policy, and institutional review processes. The implication for Consentio is that compliance cannot be hard-coded as a GDPR-only model. Instead, the platform should represent privacy obligations as configurable governance rules: consent wording, withdrawal limits, retention periods, data-residency expectations, REB/IRB approvals, and audit-reporting duties should be adjustable to the jurisdiction and institution. This design choice preserves the thesis's personal-data-sovereignty commitment while recognizing that Canadian legal authority, research ethics, and public-health mandates may define different boundaries than GDPR.

As discussed in this section, Data Sharing Networks (DSN) are an approach to PHI-sharing between different stakeholders for research. However, this area is still new and needs more literature on appropriate DG frameworks to guide researchers interested in creating DSNs (Kim et al., 2014).

## 6.5 Data Governance Requirements for Public Health Research

In (Kim et al., 2014), the authors conducted a study that utilized a triangulation method to develop DG requirements for distributed clinical research networks, which included policy analysis with experts, focus groups with patients, and interviews with institutional leaders. Their results presented 91 requirements generated from the analysis and were segmented into two categories: (i) basic requirements for all data types; and (ii) data type-specific requirements for protected health information and non-protected health information. Their work classifies protected health information as limited to datasets and identified data, and non-protected health information data as summaries and deidentified data. One point of note is that all three groups studied expressed the need for informed consent from data subjects and their right to data access, except when studies utilize deidentified non-protected health information. In conclusion, this work mapped common data governance requirements between actors and stakeholders involved in healthcare research, which served as one of the building blocks of this work's developed model.

Another work relevant to the developed model is (Marina Micheli et al., 2020), in which the authors defined emerging models of data governance that are being utilized when different actors decide to share data between themselves. Although that paper is not specifically focused on the public health domain, its formalization of each type of governance model is relevant to this work as well. Especially relevant is the personal data sovereignty model, which focuses heavily on empowering data subjects by giving them decision-making power on how their PHI are utilized by third parties. This aspect of the model is important to our governance model because power imbalances between data owners and data subjects are one of the main problems faced by public health researchers when trying to gain access to PHI from data subjects' smart devices and sensors. Table 4 below presents the data governance models mapped by the authors:

*Table 4 - Data governance models mapped by (Micheli et al., 2020b).*

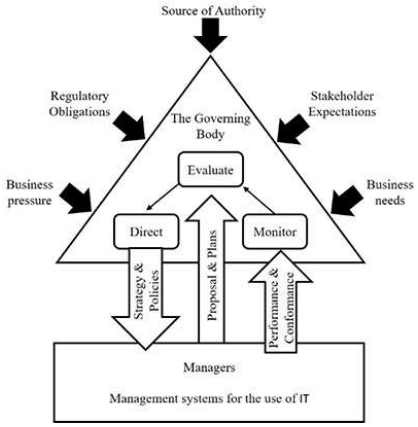
| Model | Description | Data Governance Mechanisms | Limitations |
|---|---|---|---|
| **Data Sharing Pool** | Different actors share data to fill in knowledge gaps<br>Lower costs and co-ownership stakes in the resulting dataset<br>Data is transacted as a commodity and should benefit all stakeholders<br>Horizontal approach involving data stewards and data custodians | Technical architectures, such as data sharing platforms, Application Programming Interface (API), and contracts | Exclusion of data subjects from negotiations<br>Transaction costs are high as data preparation and interoperability efforts are significant<br>There is always a "bigger" partner that ends up having more influence in the pool, thus removing part of the horizontality |
| **Data Cooperatives** | Allows involvement of data subjects<br>De-centralized data governance in which data subjects pool their data together in exchange for mutual benefits<br>Data owners control data usage, thus empowering data subjects<br>High reciprocity, all stakeholders are relevant and bound by governance rules<br>Enhances trust and transparency | Bottom-up data trusts<br>Contracts | Need to generate profit to pay for maintenance whilst profit not being the focus of the model<br>Struggles against big tach companies and their capabilities to scale |
| **Public Data Trusts** | Public actors utilize citizens' data, even data hosted by private organizations, based on a stablished trust model<br>Aggregation of different data sources to inform policy making, social innovation, and address societal challenges | Data as a public infrastructure<br>Trust building initiatives<br>Legal frameworks | Depends on public trust in public entities<br>Dependency in third party organizations to provide unbiased and independent audits |
| **Personal Data Sovereignty** | Data subjects have "almost" complete control of their data<br>Highly nationally bounded<br>Combats aggressive industry surveillance of data subjects' data<br>Increases self-determination of data subjects<br>Balances relationship between users and big tech<br>Social focused generated services | Technological Sovereignty<br>Community groups and boards<br>Private clouds and storage<br>GDPR | Dependency on data subjects IT knowledge and trust<br>Private clouds and storages are still in early stages of adoption<br>Giving the choice to share for data subjects is not enough to combat disparities in power within the current data landscape |

The personal data sovereignty governance (PDSG) model has the necessary properties to ensure that our model empowers data subjects and aligns with GDPR's data subjects' data rights protection. However, as stated in Table 4, giving people the choice to share data subjects' data does not mean that disparities are non-existent. Governance mechanisms are necessary to ensure data subjects' role in our IODG framework and protect them from power disparities as much as possible. Furthermore, PDSG's focus

on the social aspects of services provided between data subjects and data owners aligns synergistically with public health objectives of improving population health and public health policies. The PDSG model tries to diminish power imbalances between data subjects and data owners; nevertheless, it depends on data subjects' technology knowledge, trust, adoption of private clouds, and depends on stakeholders' acceptance of the IODG compliance requirements present in a DSA terms. Specifically, the IODG or DG framework ensures that a PDSG initiative will not cause liabilities to stakeholders (Hande & Mane, 2015; Marina Micheli et al., 2020; Wende, 2007).

Although both previous works discussed in this section outline important aspects and requirements of an IODG framework, they are not enough to extrapolate a new IODG framework. Rather, they serve as a requirements list and a conceptual model of a data governance initiative. We also studied high-level DG frameworks, to understand how corporate governance is implemented and maintained in real-world settings. The first DG standard studied was the ISO/IEC 38500, which outlines governance principles and guidance for a governing body of an organization, specifically, for the governance of I.T. Figure 2 below shows the ISO/IEC 38500 conceptual model and its interactions with the management, alongside sources of influence.

*Figure 2 - ISO/IEC 38500 conceptual model.*




The ISO/IEC 38500 defines three major responsibilities for the governing body of an organization, evaluate, direct, and monitor. Evaluate is a component that focus in, literally, evaluating the current and future usage of I.T. technologies. A governing body gathers data collected and processed by the Monitor component to evaluate compliance and performance of the organization data strategy. They also utilize these metrics to decide whether to include new proposals and plans in their governance framework or not. Direct assigns roles and responsibilities for the implementation of the strategies, plans, and policies defined at the governance level. It defines those who are accountable for non-compliance, low performance, and consequences for problems that impact the organization. ISO/IEC 38500 follow six principles that support the direct, evaluate, and monitor component of their framework:

1. **Principle of Responsibility**: I.T. professionals must acknowledge their responsibilities regarding I.T.'s resources and requests and should have the necessary authority to perform actions and decisions that they are accountable for.
2. **Principle of Strategy:** Preaches Business and I.T. synergy. The business's strategy takes into account IT's current and future capabilities, and I.T.'s strategy must result in meeting the business's strategy requirements.
3. **Principle of Acquisition:** Investment in I.T. decision-making needs to be transparent, balanced between cost and opportunity, and with proper knowledge of possible current and future risks.
4. **Principle of Performance:** I.T. should be "fit-for-purpose", and deliver systems that are appropriate for the task, and that takes in consideration risks, performance, and monitoring of I.T. systems.
5. **Principle of Conformance:** Requires that I.T. comply with all regulatory, contractual obligations, and standards defined by the governing body.
6. **Principle of Human Behaviour:** Requires that I.T. policies, processes and decisions take into consideration and respect human behaviour.

In (Khatri & Brown, 2010), articulate data governance as a deliberate design problem that links "information assets" (documented facts with value) to the IT assets that operationalize them, and they argue that effective governance begins by identifying the fundamental data decisions an organization must make and assigning clear accountability for making them. Their framework specifies five interdependent data decision domains, data principles, data quality, metadata, data access, and data lifecycle, where principles orient intended use, quality standards shape meaning and fitness-for-use, metadata enables consistent interpretation, access rules institutionalize permissible use, and lifecycle decisions govern creation, retention, and retirement in ways that make principles implementable through infrastructure. Central to their contribution is the "locus of accountability" concept: decision rights for each domain can be configured along a centralization–decentralization continuum, yielding a governance matrix that reflects how authority should be distributed given organizational structure and where data ownership and expertise reside (Khatri & Brown, 2010).

A complementary perspective emerges from the IT governance literature, which frames governance research within a cube defined by three questions: who is governed (the unit of analysis, from an application to an ecosystem), what is governed (IT artifacts, their informational content, or stakeholder relationships), and how governance is enacted (decision rights, formal/informal controls, and even architecture as control). This "cube" lens is useful for positioning data governance choices as inherently multi-level and mechanism-dependent, rather than as a single organizational policy layer (Tiwana et al., 2013)

Building on these foundations, (Abraham et al., 2019) Synthesize the data governance literature through a structured review and propose a six-dimensional conceptual framework that explicitly broadens scope to accommodate contemporary data environments. Their model places governance mechanisms at the core (structural, procedural, and relational mechanisms), and then specifies organizational scope (intra- vs. inter-organizational), data scope (traditional data vs. big data), and domain scope (the decision areas to which mechanisms are applied). Notably, they expand the decision domains to include data architecture and data storage/infrastructure alongside established concerns such as quality, security, lifecycle, and

metadata, and they emphasize that governance should be understood end-to-end by considering both antecedents (contingency factors and barriers shaping adoption) and consequences (value creation, risk management, and performance effects) (Abraham et al., 2019; Van Panhuis et al., 2014).

In the specific context of health data, (Winter & Davidson, 2019b), foreground the governance tensions that arise when personal health information (PHI) becomes a critical input to AI/ML innovation: governance must simultaneously protect privacy and equity while enabling legitimate secondary use for system improvement, yet scale, opacity, and cross-organizational fragmentation can strain conventional safeguards such as notice-and-consent and baseline privacy regulation. These governance pressures intersect with the well-documented practical barriers to public health data sharing as synthesized in (Van Panhuis et al., 2014), who identify a taxonomy of interacting obstacles across technical, motivational, economic, political, legal, and ethical categories. Their review highlights foundational infrastructural constraints (e.g., data not collected, not preserved, restrictive formats, language barriers, and insufficient metadata/standards), incentive and credit dynamics that discourage sharing, resource limitations and potential economic harms (e.g., tourism/trade impacts during outbreaks), and higher-level trust, policy, ownership, privacy, proportionality, and reciprocity challenges that require governance arrangements beyond purely technical fixes.

## 6.6 Methods: Application of the Governance Analytical Framework (GAF)

The basis for the creation of the DG framework was the Governance Analytical Framework (GAF) (Aeberhard & Rist, 2011; Hufty, 2008). The GAF is a practical methodology that demonstrates how governance can be used to analyse collective problems. It assumes that governance processes can be identified in any society based on observation and/or analysis from a non-normative and non-prescriptive perspective. It provides a research-based data governance development methodology, which determines how decisions are made and what social norms and institutions are created. A scoping review was conducted to identify, understand, and formalize the main actors involved in public health research, followed by the

identification of their collective problems, social norms, transactions, and nodal points so that a proper governance model could be developed.

Based on the GAF methodology, five analytical principles were utilized: the problem, the actors, the nodal points, the social norms, and the processes. The problem at stake for this work is defining a DG framework and model for public health research. Stakeholders involved in the public health research process come to DSA and DG requirements that influence social norms. Social norms guide the behaviours and actions of the actors involved and are modified over time by the collective actions and agreements of the stakeholders. The collective actions are reflected in nodal points by influencing the actors' behaviours when discussing problems, and are impacted by social norms, processes, and actors. Processes are a sequence of states resulting from the relationship between stakeholders, social norms, and nodal points. In public health research, processes are formally guided by laws, regulations, and authority figures that impact the decisions and behaviours of stakeholders and social norms at nodal points.

Although GAF is not necessarily a public health-focused framework, it is a formal and procedural manner to define and understand in-depth the complexities involved in IODG for public health research.

Research questions that guided the application of the GAF framework were:

- **Research Question 1.1**: What are the main challenges of data governance adoption by public health organizations?
- **Research Question 1.2**: Who are the actors involved in inter-organizational public health research?
- **Research Question 1.3**: What are the actors' collective problems and social norms?
- **Research Question 1.4**: What types of transactions do actors involved in inter-organizational public health research engage in? And which transactions incur directives, or power imbalances?
- **Research Question 1.5**: Can a data governance framework be extrapolated from the GAF application that could be used by multiple sub-domains of the public health research domain?

## 6.7 Defining GAF Components for the Public Health Domain

For each component of the GAF framework, state-of-the-art papers, grey literature, and standards documentation were utilized. For example, to define the actors involved in public health research, literature regarding public health and research, big data and public health, and data governance and public health were read to extract the most relevant actors (Benke & Benke, 2018; Bublitz et al., 2019; Khoury & Ioannidis, 2014; Lopez, 2010; P. Galway et al., 2016; Riordan et al., 2015; Rivera et al., 2007; Van Panhuis et al., 2014; Walport & Brest, 2011). To define actor's social norms and collective problems, papers read were regarding challenges and barriers to data governance adoption in public health research, challenges to DSA initiatives in public health, and PHI sharing privacy challenges were analysed (Benke & Benke, 2018; Frank & Di Ruggiero, 2003; Katal et al., 2013; Khoury & Ioannidis, 2014; Tse et al., 2018b; Walport & Brest, 2011; Winter & Davidson, 2019a). Finally, to define nodal points and processes papers regarding DG frameworks, DG design, and DG mechanisms were read (Abraham et al., 2019; Aisyah & Ruldeviyani, 2019; Al-Badi et al., 2018; Alhassan et al., 2019; Al-Ruithe et al., 2019; Canadian Institute for Health Information, 2020; Cheng et al., 2018; CIO Central Guest, 2017; Evren et al., 2021; Gregory, 2011b; John, 2018; Khatri & Brown, 2010; Kim & Cho, 2018; Kim et al., 2014; Li et al., 2019; Marina Micheli et al., 2020; Panian, 2010; Prukalpa, 2021; Rosenbaum, 2010; Thomas, 2010; Tse et al., 2018b; Winter & Davidson, 2019a; Wu et al., 2021). Although the defined components based on our mapping do not represent all possible actors, social norms, collective problems and processes of the entire public health research domain, the framework and methodology presented here can be extended and adapted to different use-cases and similar domains.

Next, section 6.8 will describe the results obtained after applying the GAF steps, and the mapping of actors, collective problems, social norms, transactions, and processes that were mapped as necessary to facilitate public health research initiatives. Although we will be discussing more of the GAF and its concepts, it is out of the scope of this section to provide deeper explanations of GAF concepts.

## 6.8 Results

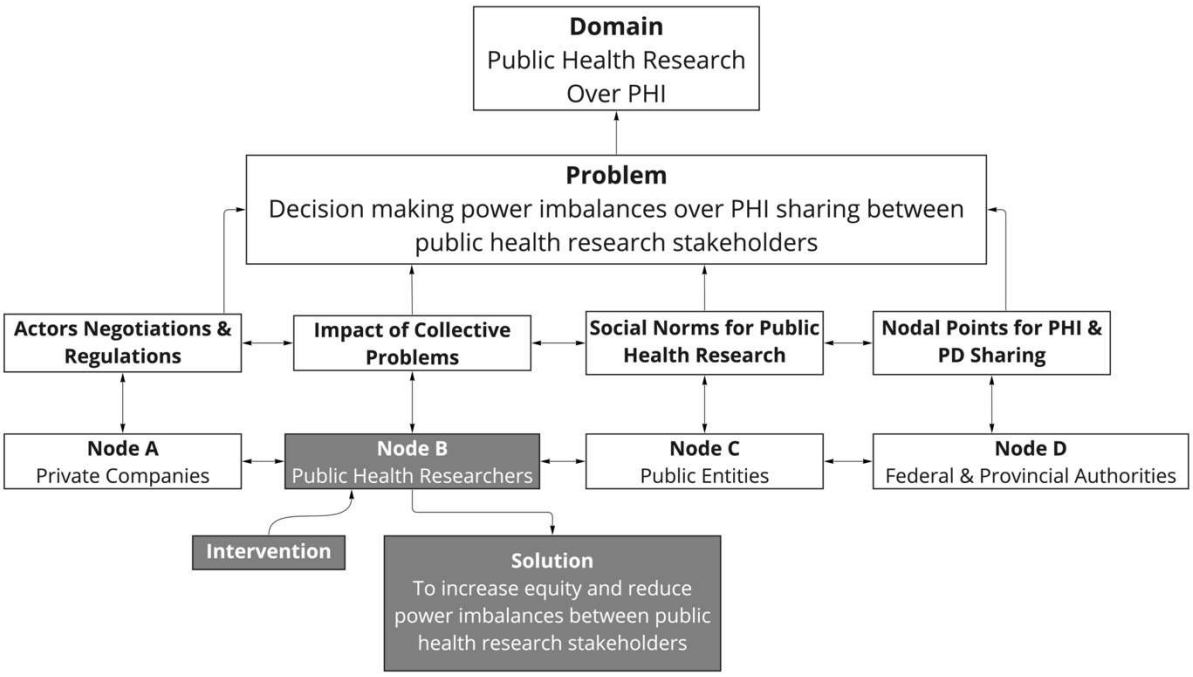
The diagrams and tables presented below illustrate the application of the GAF for the public health research domain. The first step (Figure 3) was the identification of the independent and dependent variable. The independent variables are the actors and stakeholders that possess leverage on the decision-making process of PHI data sharing with researchers, meaning that they impact dependent variables through the governance process at the decision-making level. The dependent variables are those who are impacted by the independent variables through the governance process, in this case, public health researchers. Finally, governance itself is the intermediary variable that is responsible for providing allocation of decision-making and accountability, guidelines, and policies, and to monitor compliance and performance, which aims to create the "fairest" environment between both independent and dependent variables, whilst acknowledging their power and influence. We decided to base our IODG framework on (Abraham et al., 2019; Marina Micheli et al., 2020; Schröder-Bäck et al., 2014), as initial building blocks, as it promotes more equity and less power imbalances between actors.

*Figure 3 - Independent and dependent variables of the public health research domain based on the GAF.*

| Stakeholder Management | | |
|---|---|---|
| **Independent** | **Intermediary** | **Dependent** |
| Federal Government's Laws and Regulations<br>Federal Province's Laws and Regulations<br>Private & Public Entities' Organizational Structure and Internal Objectives<br>Institutional Review Board's Compliance<br>Data Subject's Personal Believes | Personal Data Sovereignty Data Governance for Public Health Research | Public Health Researcher PHI access |

For the second step, the GAF diagram (Figure 4) is presented, showcasing the nodal points between actors and stakeholders, taking into consideration where the intervention is being applied. In Figure 3, the main intervention is being applied to node B, where public health researchers lack the means and leverage to interact with other actors to achieve their goals. Other nodal points are impacted, or directly impact nodal point B, such as node A, which represents private companies. Node A has its own social norms, internal problems and actors that comply with its organization data strategy. Any external influences, such as sharing PHI for public health research requires a negotiation interaction between node A and node B. But if a public health research involves public entities as research stakeholders or actors, node C must be included. Additionally, if PHI is not anonymized, or has meta-data capable of identifying data subjects, provincial or federal authorities must be involved, for example, an IRB could be present in node D . In this example, four actors would interact in a nodal point to negotiate which is the data governance framework that must be complied by all actors involved in order for PHI to be shared with researchers.

*Figure 4 - GAF diagram of data governance for public health research.*




### 6.8.1 Public Health Research Domain Assessment (Actors, Social Norms and Collective Problems)

The Public Health Research Domain (PHRD) includes academic researchers studying public health, public health research institutions, public companies, private companies, the federal government, and the general population. Each stakeholder possesses a unique infrastructure, corporate interests, social norms, and governance guidelines. In (Winter & Davidson, 2019b), challenges were described in balancing the increased privacy and infrastructure requirements of utilizing PHI for studies with the benefits of improving public health researchers' access to data. For example, PHI collected by Public Health Domain (PHD) stakeholders is not standardized: it is stored in its own premises and with ad-hoc technology, and under different levels of data governance maturity. Coming through an agreement to share data stored in multiple entities requires sharing of responsibilities, which, based on the type of data, becomes incrementally more complex.

Stakeholders that possess higher levels of data governance maturity, normally private companies and public entities that hold PHI, occupy positions of power and leverage over entities that possess lower levels of data governance maturity (e.g., academic researchers, public health institutions). Although it ensures proper protection of PHI, this imbalance impacts the PHD access to PHI, delaying innovations and faster progress in public health research. As mentioned in (Van Panhuis et al., 2014), iImpediments to PHI data sharing include technical barriers, such as a lack of standards and metadata, which are subsets of guidelines and policy implementation, which themselves are derived from data governance models. A flexible data governance model can be achieved if all the necessary stakeholders can create channels of communication to negotiate and create data governance models that can be used as a template for future initiatives. A flexible data governance model for public health research should serve as a baseline to be adapted by the public health sub-domain of research.

Based on the current landscape of public health research, different actors need to come to an agreement regarding a common data governance model before sensitive data can be shared. However, for a data governance agreement between actors to be possible, it is necessary to understand actors' collective problems and social norms. Identifying actors' collective problems exposes problems that actors in the same market segment have, whilst social norms help with project planning since an actor can better prepare for negotiations regarding data governance requirements.

To understand the domain of the developed DG framework, a domain scoping, including white and grey literature, was conducted to compile common collective problems and social norms for each actor identified in the GAF Diagram. Tables 5 and 6 present the complete mapping of each mapped actor and their collective problems and social norms.

*Table 5 - Governance actors and social norms in public health research.*

| Actor | Collective problems | Social norms (IDs) |
|---|---|---|
| **Public Health Researcher** | Access to PHI data; High cost of obtaining informed consent; Funding; Lack of specific IT resources; Data quality; Just enough data; IRB Compliance; Lack or insufficient data governance mechanisms | 1,2,3,4,5,6,7,8,15,16,35 |
| **Private Entity** | Ethical and privacy concerns; Users' privacy concerns; Laws and regulations compliance (liability); Lack of stimulus; Lack of accountability tools and measures; Lack or insufficient data governance mechanisms | 1,2,3,4,5,6,7,8,9,10,11,12,13,14 |
| **Public Entity** | Ethical & Privacy concerns; Laws and regulations compliance (liability); Public health research goals requirements; Lack of stimulus; Lack or insufficient data governance mechanisms | 1,2,3,4,5,6,7,8,9,10,11,12,13,14 |
| **Federal Province** | Political Agendas; Slow Pacing; Bureaucratic (red tape); Uneven Distribution of Effects; Ethical & Privacy concerns; Constitutional Compliance; Public health research goals requirements; Competing interest of funding; Lack or insufficient data governance mechanisms | 1,2,3,4,5,6,7,8,11,12,13,14 |
| **Federal Government** | Political Agendas; Slow Pacing; Bureaucratic (red tape); Uneven Distribution of Effects; Ethical & Privacy concerns (liability); Constitutional Compliance; Public health research goals requirements; Competing interest of funding; Lack or insufficient data governance mechanisms | 1,2,3,4,5,6,7,8,9,10,11,12,13,14 |
| **Data Subject** | Users' privacy concerns; Lack of specific PHI research knowledge; Lack of specific IT knowledge; Lack of stimulus; Lack or insufficient data governance mechanisms | 1,9,10,11,15,16 |
| **Institutional Review Board** | Proper bio-medical research conduction concerns; Ethical & privacy concerns; Laws and reulations compliance (liability); Public health research goals requirements; Lack or insufficient data governance mechanisms; Lack of specific IT knowledge | 8,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,32,33,34 |

*Table 6 - Social norms legend for public health research governance.*

| Id | Social norms legend (Type) |
|---|---|
| **1** | Collection of informed consent |
| **2** | Adequacy |
| **3** | Accountability |
| **4** | Data sharing agreement |
| **5** | Binding corporate rules |
| **6** | Code of conduct |
| **7** | Integrity |
| **8** | Study protocol |
| **9** | Privacy protection policies |
| **10** | PIPEDA |
| **11** | Provincial privacy laws |
| **12** | Freedom of Information and Protection of Privacy Act, Ontario's provincial public sector privacy law |
| **13** | Municipal Freedom of Information and Privacy Act, Ontario's provincial public sector privacy law |
| **14** | Personal Health Information Protection Act |
| **15** | Informed consent form |
| **16** | Informed consent process |
| **17** | Belmont principles compliance |
| **18** | Waivers of informed consent |
| **19** | Initial review requests |
| **20** | Conflict of interests |
| **21** | Certification of confidentiality |
| **22** | Board action approve |
| **23** | Board action approve with conditions |
| **24** | Board action disapprove |
| **25** | Board action defer |
| **26** | Board action pull |
| **27** | Board action update |
| **28** | Board action study renewal |
| **29** | Board actions closure |
| **30** | Continuing review forms |
| **31** | Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans |
| **32** | Division 5 of the Food and Drug Regulations; Part 4 of the Natural Health Product Regulations; Part 3 of the Medical Device Regulations |
| **33** | REB operational policy framework |
| **34** | IRB approval |
| **35** | HIPAA, GDPR |

### 6.8.2 Actor Public Health Researcher

Public health researchers, whether individuals, teams, or institutions, often lack the IT expertise to design interoperable pipelines and robust governance controls for personal health information (PHI) and personal data (PD). Proficiency in analytics tools does not translate into building access controls or audit-ready practices at the level expected by large custodians, so collaboration depends on narrow agreements that align data-sharing conditions with each actor's capacity while acknowledging power asymmetries.

### 6.8.3 Actor Private Company

Private companies act as custodians of PHI and thus bear significant liability if privacy breaches occur. Because their incentives are oriented toward profit, innovation, and risk management, their participation in public-health research tends to be conditional: sharing occurs only when the perceived benefits (e.g., reputation, tax relief, innovation alignment) outweigh potential legal and reputational costs, not as a purely altruistic contribution.

### 6.8.4 Actor Public Entity

Public entities, such as hospitals and governmental research institutes, have more constrained IT infrastructure and governance capacity than private firms, limiting their PHI access and driving reliance on public datasets or additional investment in infrastructure. Their policy-driven objectives can clash with private companies' liability-averse strategies. Relevant norms derive from laws like PIPEDA and Ontario's Personal Health Information Protection Act, combined with research protocols (e.g., informed consent, adequacy, study protocol) and data-sharing agreements (DSAs) emphasizing accountability and contractual obligations.

### 6.8.5 Actor Federal Government

In this framework, the federal government is treated as an authoritative regulator whose constitutions, institutions, and enforceable regulations set the legal conditions for PHI access and shape other actors' behaviour (Fadrique, 2019). Because new directives require other actors to adjust their governance

practices, structural power imbalances persist and cannot be resolved through interactor negotiation; thus, the federal actor is relatively static within DSAs and interorganizational data-governance (IODG) bargaining. Regulatory change may disproportionately burden smaller actors who cannot comply immediately or at all (Coe et al., 2001; Tse et al., 2018a).

### 6.8.6 Actor Canadian Provinces

Provinces are distinct regulatory arenas because PHI rules differ by jurisdiction. Although Ontario is foregrounded here, the model accommodates substitution or extension to other provinces; they share many problems with the federal government, but may participate directly in DSAs or IODG negotiations while shaping behaviour through provincial laws and regulations.

### 6.8.7 Actor Data Subjects

Data subjects are individuals whose PHI underpins public-health research. They face privacy concerns, unfamiliarity with IT or research processes, low motivation to share, and distrust in how their data will be handled. Even with established protections, participants often fear losing control once they consent, underscoring the importance of mechanisms that let them see, modify, or withdraw consent, thereby improving trust and participation (Barney & Antisdel, 2013; Fadrique, 2019; Musmade et al., 2013).

### 6.8.8 Actor Institutional Review Board

Institutional Review Boards (IRBs) enforce ethical standards and regulatory compliance in studies involving PHI. As data collection shifts from clinical settings to remote apps, sensors, platforms, and wearables, IRBs must ensure consent materials accurately represent complex data flows, re-consent provisions, and the governance safeguards needed for remote collection (McDonald, 2022; *Office of the Privacy Commissioner of Canada*, 2015; Tovino, 2017). Their oversight can reshape DSAs and IODG conditions by compelling transparency about IT infrastructure and governance maturity, sometimes generating tension when stakeholders want non-disclosure agreements or other protections.

## 6.9 Mapping of Public Health Research Domain's Transactions (GAF Transactions)

Following the GAF methodology, the analysis is structured around the problem, actors, nodal points, social norms, and processes. The problem here is PHI sharing among data subjects and public and private entities for public health research. At nodal points, actors negotiate agreements that define guidelines, policies, rules, standards, and accountabilities that make DSAs and an IODG framework feasible; these arrangements shape social norms over time and are modified through collective action. Processes are understood as sequences of states that arise from these interactions and are often formalized through law, regulation, and institutional authority.

Actors do not share equivalent governance capacity, incentives, or constraints, and factors such as business model, jurisdiction, data sensitivity, and organizational relevance influence what governance is feasible. Transaction mapping, therefore, supports practical governance design by identifying likely power imbalances, predictable conflicts of interest, and appropriate actor roles. Table 7 maps transactions into the four GAF categories: negotiation, directive, distribution, and reciprocity, with reciprocity drawing on Mauss's gifts and counter-gifts theory (Aeberhard & Rist, 2011; Hufty, 2008). Table 8 then provides examples of transactions between actors, and the framework requires IODG members to review and adapt these defaults to fit other domains, actor cohorts, data types, and legal contexts.

*Table 7 - Actor-to-actor governance transaction typology.*

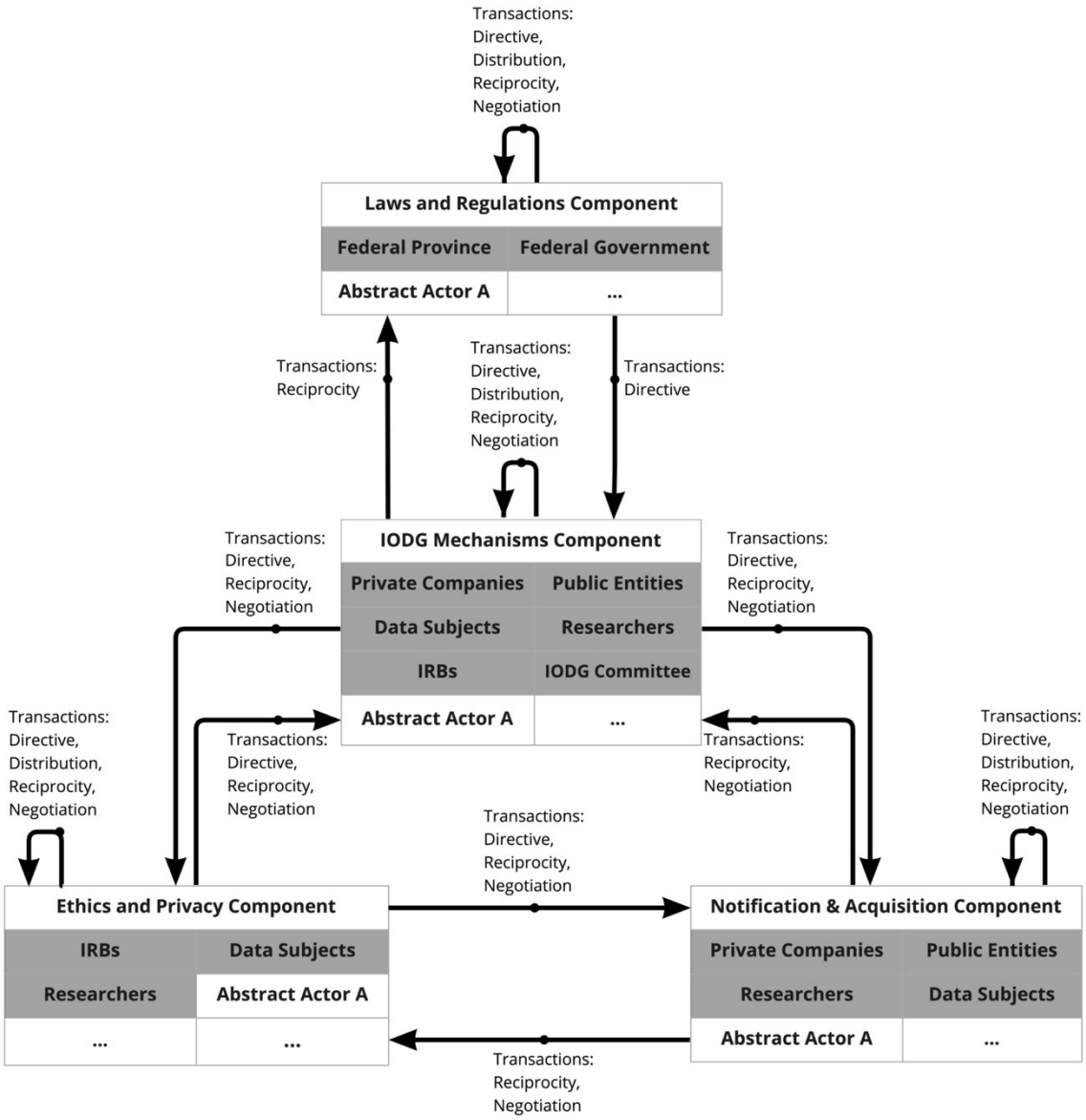
| Actor (responsibilities) | Negotiation transactions | Directive transactions | Distribution transactions | Reciprocity transactions |
|---|---|---|---|---|
| **Data subjects (provide/deny informed consent; manage PHI access; comply with research directives; comply with laws and regulations)** | Consent form negotiation; Personal data rights negotiation; Results/Benefits negotiation | Follow research interventions and guidelines | Acquiring compensation/services; Knowledge acquisition; Health improvement | Disease cure and treatments; Improved public health policies and interventions |
| **Public entities (manage PHI access, sharing, and processing; comply with DG requirements; comply with laws and regulations)** | Consent form negotiation; Personal data rights negotiation; Security and Privacy negotiation; Results/Benefits negotiation; Internal strategy negotiation; Data Governance negotiation; Funding and resources negotiation | Provide means to access data; Ensure Data Subjects' data rights; Maintain PHI integrity; Maintain proper role-based access to PHI; Allocate appropriate resources; Provide support to researchers; Ensure internal goals; Support IT and/or benefits generation | Distribution of knowledge/services to data subjects; Distribution of KT to other stakeholders; Distribution of funding; Generation of a new public health knowledge base; New public health interventions and policies | Access to Data PHI; Access to resources (funding & infrastructure); General population appreciation/recognition; Social services; Ethical and responsible research processes conducted; Innovation and/or new insights (for public health); Improvement of public image |
| **Researchers (research and acquisition of PHI for research; comply with laws and regulations; comply with IRB directives; maintain proper data governance)** | Consent form negotiation; Data access and rights negotiation; Security and Privacy negotiation; Results/Benefits negotiation; Data Governance negotiation | Ensure proper research standards and ethics; Categorize and classify PHI and PD; Ensure Data Subjects' data rights | Distribution of KT to other stakeholders; Innovation and/or new insights (for public health); Scientific publications | Access to PHI and data; Academic recognition; Research conduction; Scientific publications |

*Table 8 - Illustrative governance transaction scenarios.*

| Example | Negotiation transactions | Directive transactions | Distribution transactions | Reciprocity transactions |
|---|---|---|---|---|
| **Example #1** | Researcher ↔ Private Company (Type: Giver; Request: Innovation and/or new insights from data); Researcher ↔ Private Company (Type: Receiver; Condition: Access to data subjects' data) | Researcher ↔ Public Entity (Type: Giver; Directives: Ensure proper research standards and ethics; Categorize and classify PHI and PD; Ensure Data Subjects' data rights); Researcher ↔ Public Entity (Type: Receiver; Distribution: Funding; New public health knowledge base; New public health interventions and policies) | Researcher ↔ Public Entity (Type: Distributor; Distribution of KT to other stakeholders; Innovation and/or new insights (for public health); Scientific publications); Province (Distribution: Generation of new public health knowledge base; New public health interventions and policies; New laws and regulations) | Data subject ↔ Researcher (Type: Giver; Gift: PHI and PD); Data subject ↔ Researcher (Type: Receiver; Counter gift: Better public health interventions; New treatments for diseases) |
| **Example #2** | Researcher ↔ Private Company (Type: Receiver; Request: Data subjects' data); Researcher ↔ Private Company (Type: Giver; Condition: Informed consent; Data governance guidelines) | Researcher ↔ Public Entity (Type: Receiver; Distribution: Maintenance of proper role-based access to PHI and PD; Allocate appropriate resources; Support to researchers); Researcher ↔ Public Entity (Type: Giver; Directives: Distribution of KT to other stakeholders; Innovation and/or new insights (for public health); Scientific publications) | Province (Distribution: Generation of new public health knowledge base; New public health interventions and policies; New laws and regulations) | Data subject ↔ Researcher (Type: Receiver; Gift: Experimental treatment); Data subject ↔ Researcher (Type: Giver; Counter gift: Academic recognition; Research conduction; Scientific publications) |

Finally, after finalizing the mapping from the actors' transactions, and based on a review of available analytical governance literature (Allen et al., 2021; Hufty, 2008; Kim et al., 2014; Marina Micheli et al., 2020)The governance framework for public health research has been designed. Below, Figure 5 showcase the framework's model with its actors and appropriate transactions.

*Figure 5 - Personal Data Sovereignty Governance Framework for Public Health Research.*




The "Personal Data Sovereignty Governance Model for Public Health Research Over PHI" treats data subjects as the ultimate decision-makers over the use of their data by researchers and third parties. The model is organized into components, each containing fixed actors (mapped to public-health research) and optional abstract actors that can be added depending on the complexity of the IODG initiative.

### 6.9.1 Laws and Regulations Component

This component houses federal and provincial governments (in the Canadian context) as external actors that do not participate directly in governance but instead create laws, regulations, and standards and monitor compliance. The link to the IODG component is primarily directive: new regulations shape social norms and behaviours; the reciprocal transaction involves achieving public objectives such as privacy protection, accountability, and improved health outcomes.

### 6.9.2 Inter-Organizational Data Governance Mechanisms Component

The IODG Mechanisms component is the framework's core, containing fixed actors (e.g., private companies, public organizations, data subjects, researchers, IRBs, and an elected IODG committee). Drawing on data-governance literature (Abraham et al., 2019; Alhassan et al., 2016; Calder, 2019; Khatri & Brown, 2010; Marina Micheli et al., 2020; Thomas, 2010)It specifies decision rights, accountabilities, roles, and governance mechanisms to monitor compliance across all members. The component exchanges directives (policies and guidelines), negotiations (adaptations to requirements or infrastructure), and reciprocity (benefits such as data-strategy outcomes and equitable relations) with the Ethics and Privacy and Notification and Acquisition components.

### 6.9.3 Ethics and Privacy Component

Comprised of IRBs, public-health researchers, and data subjects, the Ethics and Privacy component ensures that IODG guidelines protect data-subject rights and adhere to biomedical research standards. It implements IODG policies while safeguarding consent and privacy (with regulations like the GDPR as guiding principles) and interacts with the IODG Mechanisms component through negotiations and reciprocity to reflect ethical requirements in governance practice. It issues directives to the Notification and Acquisition component to guarantee privacy and ethical standards are respected in data-sharing activities.

### 6.9.4 Notification and Acquisition Component

This component includes data subjects, researchers, private companies, and public organizations engaged in the acquisition and notification of PHI for research. It negotiates the conditions under which PHI can be shared and ensures reciprocity (e.g., enhanced datasets, knowledge transfer, tax incentives) but lacks directive authority over research protocols and governance; those powers reside in the IODG committee. Negotiation protects each actor's objectives: private/public companies manage internal goals and risk, researchers seek access, and data subjects retain sovereignty.

### 6.9.5 Self-Directed Transactions

Each component has internal transactions, directives, negotiation, reciprocity, and other forms that govern interactions within its domain, for example, IRBs direct researchers and data subjects within the Ethics and Privacy component. Mapping these internal flows helps identify power imbalances and informs where nodal-point negotiations are needed. The subsequent section uses this mapping to develop a macro-level generic IODG model and to identify where actor interactions at the IODG committee must occur to reach consensus.

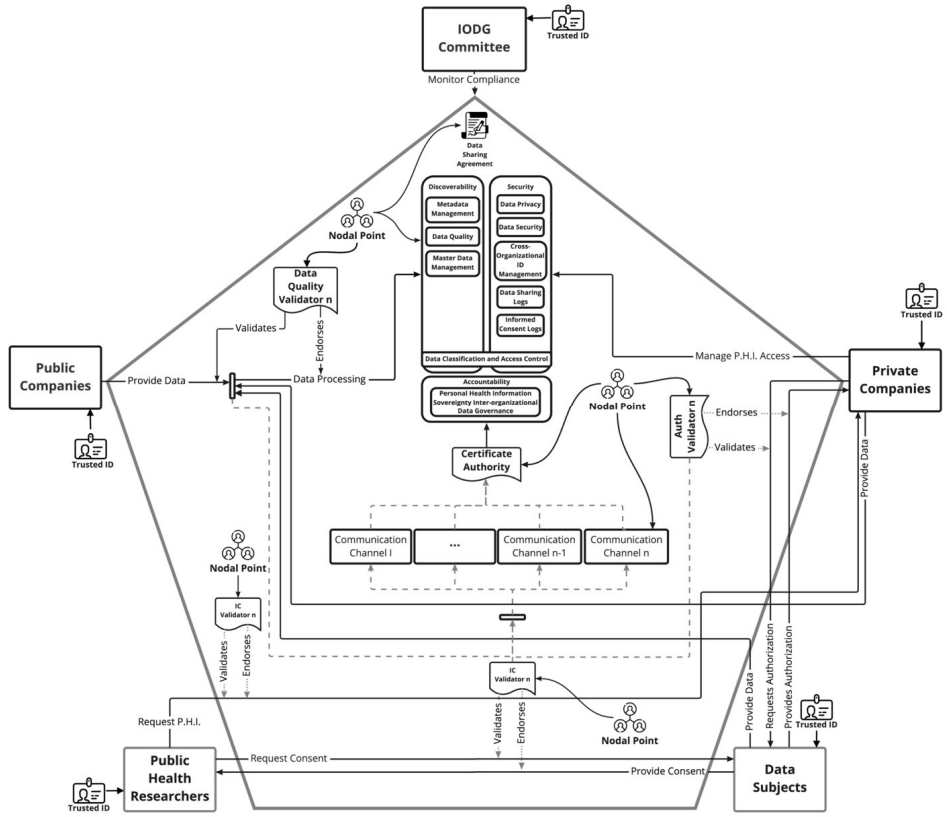
## 6.10 Personal Data Sovereignty Inter-Organizational Data Governance Model for Public Health Research

With the framework complete, the next step is to model how all actors would interact during the IODG initiative. This helps identify the topics and challenges that must be discussed and resolved at nodal points and, ultimately, reflected in the IODG framework. It also helps determine which actors should be involved at these nodal points, based on the subject's location. This model also serves as a basis for identifying where governance controls and monitoring should be allocated.

Figure 6 should be read as a high-level map rather than as a detailed implementation diagram. Its key point is that personal data sovereignty requires several linked governance layers: data-subject decisions, researcher responsibilities, ethics and institutional approvals, public/private data custodians, and audit

mechanisms that make consent-state changes traceable across organizations. The detailed labels are less important than the relationship among these layers, which is what Chapter 7 translates into platform controls.

*Figure 6 - Personal Data Sovereignty Inter-Organizational Data Governance Model for Public Health Research*




Based on the actors present in the components of the IODG framework (Figure 5). The model above was created to showcase which and where decision-making, accountability, and processes needed to be agreed upon by the IODG committee to conduct PB research over PHI. It also provides, in a non-technical and high-level way, part of the IT infrastructure needed to support the IODG initiative showcased by the model. Composing the IT infra-structure needs is a common certificate authority, which issues and manages credentials that can be used to authenticate valid members of the IODG initiative, communication channels for private communications between all or a subset of the IODG members, a common repository, that can be accessed only by members of the IODG, that holds data sharing history between actors, and location

where PHI is being stored so that other member knows which actor to request PHI data from, and what type of data processing happens before and after PHI data is stored in data silos.

Regarding actors' interactions, each request and delivery transaction between actors must be done through agreed-upon communication channels. The same transactions must be validated by the elected authority in both directions. Validation for a request is to ensure no unauthorized communication between actors, to ensure that the request is sound and complies with the IODG requirements. When a response to a request is sent back to an actor, an endorsement from an elected authority should be added to the response before returning it to the sender. Both steps of validation and endorsement are important to ensure accountability and transparency between members of the IODG initiative. Moreover, once all topics that need to be addressed at the appropriate nodal points are mapped, they can be grouped into a DSA that can be approved by the IODG committee and complied with by all members.

## 6.11 Research Questions

This section uses the Governance Analytical Framework (GAF) to condense the section's mappings into direct answers to RQ 1.1–1.5, linking the identified problems, actors, norms, nodal points, and processes to an operational, personal-data-sovereignty approach for inter-organizational PHI governance.

### 6.11.1 RQ 1.1 — What Are the Main Challenges of Data Governance Adoption by Public Health Organizations?

Data governance adoption is constrained primarily by uneven organizational maturity, with many public health research settings lacking the controls and capacities expected by PHI custodians, thereby increasing the likelihood of either overly restrictive sharing or unsafe practices. This gap is reinforced by inconsistent standards, weak metadata, limited data-preparation capacity, fragmented incentives, and jurisdictional variation, while cross-boundary uncertainty about decision rights and accountability raises transaction costs. IRBs face an added burden of communicating complex digital infrastructures and re-consent pathways without slowing studies to impractical levels.

### 6.11.2 RQ 1.2 — Who Are the Actors Involved in Inter-Organizational Public Health Research?

The core actors include researchers and their institutions seeking PHI access; custodial entities in public and private sectors that control PHI and bear liability; regulators at federal and provincial levels that impose overarching constraints; data subjects who exercise consent and withdrawal rights; and IRBs that translate legal and ethical requirements into study-level conditions. Although projects may add actors, this set provides a stable template for analyzing inter-organizational PHI governance.

### 6.11.3 RQ 1.3 — What Are the Actors' Collective Problems and Social Norms?

Actors face distinct collective problems and operate under norms that shape what they consider acceptable to share. Researchers are constrained by limited governance and software capability; private companies are shaped by liability avoidance and strategic incentives; public entities face infrastructure limits and statutory duties; regulators must protect privacy while enabling beneficial research; data subjects prioritize trust, understanding, and revocability; and IRBs must update oversight practices for digital data collection while maintaining participant protection. These misaligned norms explain why simple "open data" expectations often fail in PHI contexts.

### 6.11.4 RQ 1.4 — What Types of Transactions Exist Among Actors, and Which Entail Directives or Power Imbalances?

Actors face distinct collective problems and operate under norms that shape what they consider acceptable to share. Researchers are constrained by limited governance and software capability; private companies are shaped by liability avoidance and strategic incentives; public entities face infrastructure limits and statutory duties; regulators must protect privacy while enabling beneficial research; data subjects prioritize trust, understanding, and revocability; and IRBs must update oversight practices for digital data collection while maintaining participant protection. These misaligned norms explain why simple "open data" expectations often fail in PHI contexts.

### 6.11.5 RQ 1.5 — Can a Framework Be Extrapolated from the GAF Application for Multiple Public Health Sub-Domains?

A reusable framework can be extrapolated by separating stable governance components from domain-specific workflows. The proposed personal-data-sovereignty framework integrates regulatory directives, ethics and privacy requirements, inter-organizational governance allocation, and operational notification and acquisition processes, supported by shared infrastructure for authenticated interaction and accountability. Because these components are modular, the framework can be adapted across public health sub-domains by changing local policies and workflows without altering its core protections and decision-rights structure.

## 6.12 Discussion

Using the Governance Analytical Framework (GAF) to move from descriptive mapping of PHI sharing to a design for a Personal Data Sovereignty Inter-Organizational Data Governance (IODG) framework positions governance as orchestration rather than another checklist of best practices. The framework coordinates decision rights, accountability and oversight among researchers, custodians, regulators, IRBs and data subjects, treating PHI transactions as auditable procedures across organizational boundaries (Mathew, 2024). It clarifies that directive authority belongs to democratically accountable regulators and should not reside at the operational request layer; revocable, auditable participant control stabilizes collaboration among unequal actors (Mathew, 2024).

### 6.12.1 From Analysis to Orchestration

The central contribution is orchestrating roles: researchers' access and methods are shaped by custodians, regulators and data subjects, each under distinct norms and liabilities. A structured, multi-tiered governance framework, incorporating legal, governance and technical tiers with audits and encryption, supports this cross-boundary coordination (Mathew, 2024). Control must be revocable and traceable through

mechanisms such as platform-based consent management and blockchain interaction histories (Welzel et al., 2025).

### 6.12.2 The Sovereignty Turn

Elevating personal data sovereignty treats individual control as a primary entitlement rather than a residual privilege. For many participants, dynamic consent models can cause "consent fatigue" because of frequent, detailed requests (Welzel et al., 2025)Yet evidence shows that transparency and active (opt-in) consent mechanisms increase willingness to share health data. Cross-border storage exposes data to inconsistent legal regimes and state surveillance, making it vital to give users more control over data flows (Mathew, 2024). Sovereignty must also account for inequities in digital literacy and connectivity; simplified interfaces, digital-literacy training and co-development with marginalized communities are essential (Welzel et al., 2025). Indigenous data sovereignty underscores that communities must control how data about them is collected, accessed and used (Strayer & Grebliunas, 2024), suggesting default practices such as minimization, purpose limitation and community oversight to avoid reinforcing mistrust.

In this thesis, personal data sovereignty is used as a design orientation rather than an absolute claim that individuals can control every downstream use of data. The framework centers participants as first-class governance actors, but it also recognizes limits imposed by ethics approvals, retention duties, de-identification, public-health obligations, and cross-jurisdictional privacy law. This framing aligns with the evaluation limitations discussed later in the thesis: a sovereignty-oriented platform must make rights visible and actionable while avoiding the assumption that all users have equal legal knowledge, technical confidence, or bargaining power.

### 6.12.3 Constraining Power Without Paralyzing Practice

The design deliberately denies directive power at the Notification and Acquisition layer, preventing dominant custodians from imposing unilateral terms. Directive authority is centralized in the IODG mechanism, which validates, endorses and logs transactions. To avoid procedural inertia, service-level

objectives and automated policy checks can speed validation; emergencies still prioritize regulators' directives to balance privacy and public-health reciprocity. Strong governance frameworks and service contracts delineating compliance duties help manage ambiguity around shared responsibility in global cloud environments (Mathew, 2024).

### 6.12.4 Evaluation and Evidence

Evaluating this conceptual framework requires legitimacy, performance and substantive outcomes. Success indicators include whether data subjects perceive governance as fair and comprehensible; whether consent modifications and enrolment patterns show sustained engagement; whether service-level objectives for fulfilling legitimate requests are met; and whether unauthorized reuse or breaches are detected through robust logs and audits (Mathew, 2024; Tang, 2023). Transparent consent management and pseudonymization/anonymization techniques can enhance trust and willingness to share (Welzel et al., 2025), so monitoring trust and equity outcomes is critical.

### 6.12.5 Interoperability, Standardization and Politics of Translation

Heterogeneity across standards, platforms and vocabularies necessitates translation devices. Machine-readable policy artifacts (encoding consent conditions and purpose limitations) enable consistent enforcement, while ledgered interaction histories provide auditable records of requests, endorsements and data processing. Consent tracking, pseudonymization and anonymization must interact with these policies to ensure both privacy and regulatory compliance. Decentralized technologies such as blockchain, self-sovereign identity and de-identified tokens offer tamper-proof audit trails and user-controlled consent management. Adoption will require pooled funding and incentives to overcome deficits in metadata quality and preparation capacity (Welzel et al., 2025).

### 6.12.6 Extensibility and Adaptability

The framework is modular: core components remain stable, while actor sets, consent conditions and evaluation measures adapt to specific contexts. Anchoring the design in rights-preserving regulation (e.g.,

GDPR-like rights, PIPEDA) and emphasizing data residency and local compliance facilitate cross-jurisdiction fit (Mathew, 2024). Extensibility must avoid "governance theatre"; accountability requires audits and enforceable sanctions, and smaller institutions may need graduated compliance supported by shared services.

## 6.13 Limitations and Boundary Conditions

This design remains conceptual and not yet empirically validated; additional actors (Indigenous governance bodies, community organizations, intermediaries, insurers) may shift decision points. There is a risk that organizations appropriate sovereignty language without changing practice. Independent audits, community oversight and calibrated sanctions are therefore essential. Because cross-border regulations create uneven compliance burdens and digital literacy gaps persist, staged support and capacity-building will be needed (Mathew, 2024; Tang, 2023; Zhang & Liu, 2010).

## 6.14 Pathways to Implementation

Implementation should occur in phases. Phase one establishes a small IOGM, publishes a rulebook for decision rights, consent templates and logging requirements, and pilots de-identified data sharing with IRB co-design. Phase two expands to identifiable PHI where lawful, increases consent granularity, and normalizes audits and transparency reporting. Phase three federates multiple IOGMs across domains or provinces using portable policy artifacts and mutual recognition of validations, supported by shared tooling and standardization incentives. Throughout, capturing learning via transaction records and shifting IRBs toward co-designing enforceable constraints will be crucial (Welzel et al., 2025).

## 6.15 Relevance

The framework reframes inter-organizational PHI sharing as structured orchestration of authority, accountability and reciprocity through validation, endorsement, logging and machine-readable policies, making collaboration predictable and auditable. It repositions IRBs as co-designers of operational constraints, embedding ethical acceptability into data flows rather than static paperwork. The promise is

lawful, transparent access for researchers, clear liability management for custodians and regulators, and enforceable control for data subjects. The principal risks are over-promising, under-resourcing and divergence between formal rules and lived practice; therefore, incremental rollout and transparent measurement are integral governance requirements (Cheng et al., 2018; Mathew, 2024; Tang, 2023; Tarrant et al., 2009; Thorogood et al., 2017).

## 6.16 Conclusion

This work objective is to provide the public health research domain with an IODG framework based on the GAF methodology that can be used as a basis for new IODG initiatives. We focused on empowering both public health researchers' and data subjects' right to access PHI data by emphasizing the data sovereignty aspect of our framework. To achieve this, we highlighted the need for an IODG framework for the public health domain, given the increased use of PHI in research, particularly due to a lack of DG maturity or motivation to implement DG in research institutions. A lack of understanding of the public health domain among private and public organizations also creates barriers to PHI sharing, and public health researchers need a better understanding of data custodians' domains. Data subjects should also be involved in the processes and given greater equity alongside public health researchers. We applied the GAF methodology to map the problem, identify where interventions are needed, map actors, social norms, collective problems, their transactions, and formalized an IODG framework in which major actors in public health research are allocated to the appropriate components based on their roles, decision-making ownership, and accountability. The IODG framework is also extensible, allowing actors to be added or removed based on the domain where it is being applied. New actors are added if the appropriate GAF methodology is followed, and their allocation into the framework respects the framework's main objective.

We provided a model based on the framework that shows where key nodes are in the IODG initiative and, at a high level, which IT infrastructure is needed to support it. This work also serves as a discussion piece on the responsibilities of each actor in the framework and what they ought to provide to each other to improve public health research outcomes, data subjects' data rights, and the creation of new

IODG initiatives. Future work includes interviews with mapped actors to evaluate the framework's feasibility and, eventually, the implementation of the framework in a real-world public health research context scenario.

# 7 Translating Data Governance Concepts into a Working Dynamic Informed Consent Management Platform

## 7.1 Introduction

This section translates Section 6's data-governance framework, articulating autonomy, accountability, transparency, equity, and data sovereignty, into a verifiable software artifact, Consentio, for dynamic informed consent in public-health research. The contribution is deliberately end-to-end: governance constructs are mapped to concrete requirements and role permissions; these are made explicit in a use-case diagram (stakeholder capabilities and boundaries of interaction), rendered as a class diagram (domain entities and associations), constrained by a state diagram (legal lifecycles and transitions), formalized in a propositional-logic specification (machine-checkable invariants), operationalized in an interface layer (guards, validators, and auditable actions), and synthesized in a discussion of architectural and empirical implications. In short, the section demonstrates how normative commitments become executable system behaviour that is safe by construction, auditable by default, and empirically observable (Abraham et al., 2019; Alhassan et al., 2019; Allen et al., 2021; Al-Ruithe et al., 2019; Holmes et al., 2014; Li et al., 2019; McMahon et al., 2019; Pedro & Morita, 2022; Tiwana et al., 2013).

Section 7 presents the implementation at two levels: a high-level account of how governance obligations become platform controls, and a reproducibility layer that records the detailed matrices, diagrams, variables, and checks used to build Consentio. The main controls are approval gates, participant consent and withdrawal workflows, role-based access, audit logging, and participant-facing transparency features. Readers should treat the detailed implementation artifacts as support for those controls rather than as the central argument of the chapter.

## 7.2 Motivation

Despite widespread enthusiasm for digital consent, practice remains characterized by ambiguity, inconsistent enforcement, and weak audit trails. Three gaps motivate this section:

**From principles to operations**: Section 6 defines who may do what, when, and under which obligations; however, prose alone does not prevent illegal states (e.g., collecting data while a study remains in draft) nor guarantee consistent interpretation across teams and deployments.

**From requirements to proofs**: Ethical and regulatory constraints must be both human-readable and machine-checkable. Encoding gates such as $So \rightarrow (Ia \wedge Pa)$ (a study may be ongoing only if IRB and PI approvals hold) and $Dshare \rightarrow (Pg \wedge \neg Pr \wedge Da)$ (sharing requires active, non-revoked consent and anonymization) as logic invariants allows pre-deployment verification, continuous testing, and runtime monitoring.

**From logic to lived UX**: Users experience governance through interfaces. If invariants do not drive the UI, illegal transitions can still be reached. Binding guards and validators directly to the formal rules ensures that participants, researchers, PIs, and auditors can only traverse valid paths, while each material action emits an audit-ready event (and, where configured, a tamper-evident ledger receipt).

Addressing these gaps yields three benefits to the thesis: (i) semantic fidelity between governance and code; (ii) stronger internal validity for empirical outcomes (e.g., consent latency, re-consent acceptance, withdrawals), because measures are collected only within legal state spaces; and (iii) reproducibility and accountability, through explicit traceability from policy → rule → implementation → audit record.

## 7.3 Specific Aims

The specific aims of this section translate the governance framework developed in Section 6 into enforceable system behaviour and evaluable software artifacts. They structure the work from governance-to-requirements mapping and unambiguous formal specification, through interface-level enforcement and auditability, to the delivery of an MVP suitable for empirical evaluation. Collectively, these aims operationalize personal data sovereignty by making approval, consent, sharing, and accountability constraints both machine-checkable and demonstrably implemented.

### 7.3.1 Aim 1 – Operationalize the Governance Framework

The goal is to map structural roles (actors and duties), procedural steps (approval gates and re-consent triggers), and relational norms (accountability, reciprocity, delegation) into concrete software controls. Evidence comes from a use-case diagram mapping stakeholder capabilities and interaction boundaries, a class diagram enumerating entities such as *Study*, *ConsentTransaction*, *StudyParticipants* and *Asset*, and a traceability matrix linking governance clauses to technical requirements (Al-Ruithe et al., 2018; M Micheli et al., 2020; Tse et al., 2018a). Together, these artifacts ensure that duties and decision rights defined in Section 6 translate into auditable system functions.

### 7.3.2 Aim 2 – Specify Legal Behaviour Unambiguously

A detailed state diagram separates administrative staging (e.g., "Stopped Study") from runtime suspensions ("Study Paused") and terminal conditions ("Study Ended"). Formal behaviour is then expressed as propositional-logic invariants with first-order extensions (e.g., "every enrolled participant must have been invited"), producing machine-checkable guards (Assale et al., 2019; Cocanour, 2017; Kaye et al., 2015a; Musmade et al., 2013). These invariants clarify permissible transitions and explicitly define the legal semantics of PHI studies.

### 7.3.3 Aim 3 – Implement Enforcement via Interfaces

The propositional invariants are enforced as route guards, component-level validators and workflow constraints in an Angular application. Each material action, approval, consent capture, re-consent, sharing, pausing, stopping and ending, triggers an audit event and, optionally, writes a verifiable receipt to a ledger. This approach ensures that interactions remain within predefined paths and that all state changes are logged transparently (Jaiman & Urovi, 2020; Omran et al., 2009; Velmovitsky et al., 2020; Z. Wang et al., 2020; Zhang et al., 2017; Zheng et al., 2018).

### 7.3.4 Aim 4 – Deliver an MVP for Sections 8 and 9 Evaluation

The team assembled a containerized, extensible platform capable of instantiating studies, obtaining dual approvals, publishing, issuing and revoking dynamic consents, messaging participants and generating audit queries. Deployment scaffolding supports forthcoming usability and performance studies, ensuring that the minimum viable product meets research requirements.

### 7.3.5 Aim 5 – Answer Research Question 2

A ledger-backed transcription method is engineered to map governance rules into a tamper-evident audit layer. Approval and consent rules are expressed as runtime predicates; multi-party approval (e.g., IRB ∧ PI) is enforced through policy checks; roles are managed with federated identity; sensitive data is partitioned into private scopes; and signed, queryable events are emitted to verify correctness, privacy and performance. Although the dissertation demonstrates one implementation using a permissioned distributed ledger, the method is substrate-agnostic.

## 7.4 Methods

This section details the methodological stack that translates the governance principles articulated in Section 6 into enforceable software behaviour and evaluable research artifacts. The approach progresses from policy interpretation to formal specification and implementation, then to auditability and evaluation. Specifically, we (Method 1) map governance clauses to verifiable requirements, (Method 2) model domain entities so that governance semantics become first-class objects, (Method 3) specify behaviour as a state machine, (Method 4) encode and verify safety invariants, (Method 5) enforce rules in the user interface, (Method 6) establish audit and observability with a realistic deployment, (Method 7) scaffold evaluation and link findings to discussion, and (Method 8) provide a substrate-agnostic, ledger-backed transcription layer that preserves provenance while respecting privacy.

### 7.4.1 Method 1: Governance-to-Requirements Mapping

Governance clauses are decomposed into testable requirements and bound to stakeholder capabilities and system controls. For instance, IRB approval is treated as a precondition, while participant withdrawal triggers global revocation. A use-case diagram expresses permissible actions for researchers, principal investigators, IRBs and participants, and a traceability matrix links each governance clause through its enforcing guard to its corresponding test, ensuring demonstrable compliance (Belli et al., 2024; Tang, 2023).

### 7.4.2 Method 2: Domain Modelling (Class Diagram)

A class model encodes entities such as *Study*, *DynamicConsentForm*, *ConsentPrivacyQuantificationScore*, *DataPrivacy*, *StudyOutcome*, *StudyVersion*, *StudySuspension*, *StudyParticipants*, *Device* and *User*. Treating consent, privacy, approval and suspension as first-class types allows precise constraints (e.g., automatic invalidation of consent when a study is paused). Aligning storage structures with audit needs enables the reliable reconstruction of the state and the justification of decisions (Welzel et al., 2025).

### 7.4.3 Method 3: Behavioural Specification (State Diagrams)

The system's lifecycle is modelled as a finite-state machine: *Idle* → *Submitted* → (*Rejected* ↔ *Revision*) → *Approved* → *Stopped* → *Started* ↔ *Paused* → *Ended*. *Stopped* (published but not active) is distinguished from *Paused* (a temporary halt during active collection), and *Started* is gated by dual approvals and, where applicable, successful ledger registration. Explicit transition guards reduce ambiguity and illegal state changes (Lange et al., 2006; Oldevik & Berre, 1998; Selic, 1998; Simons & Wirtz, 2007).

### 7.4.4 Method 4: Formal Verification Layer

Safety invariants and admissible transitions are encoded as propositional formulas with selective first-order quantification. Examples include:

- $S_o \rightarrow (I_a \wedge P_a)$ (ongoing data collection requires IRB and PI approvals);

- $S_d \rightarrow (\neg R_o \wedge \neg D_o)$ (no recruitment or data collection is allowed in draft);
- $D_share \rightarrow (P_g \wedge \neg P_r \wedge D_a)$ (sharing requires active consent, no prohibition and required anonymization);
- $\forall p\ (P_e(p) \rightarrow P_i(p))$ (every enrolled participant was invited). These formulas are compiled into unit and property tests and runtime monitors; each invariant is attached to a UI guard so violations are proactively prevented and logged deterministically (Epstein, 1990; Zhang et al., 2004).

### 7.4.5 Method 5: Interface Compliance (Angular)

The user interface mirrors the reactive state's logic vocabulary. Route guards and component-level validators enforce invariants; any illegal action produces deterministic feedback and emits an audit event with an optional ledger receipt. Couplings include automatic publication of the Dynamic Consent Form upon study publication, automatic invalidation of consent upon pause/stop/end, and mandatory re-consent (with a refreshed CPIQ) after protocol or version changes. Accessibility and security are ensured through WCAG patterns, role-based access control and least-privilege defaults (Welzel et al., 2025)

### 7.4.6 Method 6: Audit, Observability and Deployment

An append-only audit trail records all state changes, approval, publication, consent, withdrawal, and sharing, with stable identifiers that support reconstruction. A configurable ledger provides tamper-evident receipts for approvals and consents, with retries and fail-safe termination when persistence fails (Ullah et al., 2024). Observability includes metrics such as blocked actions by rule, consent latency, re-consent acceptance rates and withdrawal dynamics. The reference deployment uses containerized services and an Angular front end, hosted on Azure, to support the evaluation of Sections 8 and 9.

### 7.4.7 Method 7: Evaluation and Discussion Linkage

Enforcement occurs at the user-interaction layer, so measurements reflect only legal states. The concluding discussion synthesizes how the mapping, models, logic and interfaces jointly increase compliance and

auditability, reduce ambiguity and enable reproducible assessments of trust and usability (Abraham et al., 2019; Alhassan et al., 2019; European Parliament and of the Council of 27 April 2016, 2016; Marelli et al., 2020; Zhang et al., 2004). This positions the platform for Sections 8 and 9 studies and informs the roadmap for principal investigator/IRB and third-party dashboards.

### 7.4.8 Method 8: Substrate-Agnostic Ledger-Backed Transcription

Audit "truth" is treated as a portable layer: domain rules are captured once as executable policies and mirrored as verifiable events and predicates on the ledger used (e.g., Fabric, Corda, or Besu). The method uses open models for consent records and provenance, federated identity for role-scoped actions and interoperability tooling so proofs and receipts remain usable across chains and systems (Ullah et al., 2024).

- Rule Capture to Executable Predicates: Invariants such as $S_o \rightarrow (I_a \wedge P_a)$, $S_d \rightarrow (\neg R_o \wedge \neg D_o)$ and $D_share \rightarrow (P_g \wedge \neg P_r \wedge D_a)$ are implemented as enforceable predicates within the application's policy engine and mirrored in the audit layer; state-changing actions must invoke these predicates or be rejected.
- Multi-Party Control and Endorsement: Dual or multi-party approvals require cryptographic endorsements (e.g., co-signatures from IRB and PI) before transitions are committed.
- Identity and Roles: Federated identity (PKI or OIDC) binds roles (researcher, PI, IRB, auditor, participant) to invocation rights; access control lists gate privileged functions.
- Data Partitioning and Privacy: Sensitive artifacts remain off-chain in encrypted stores, while cryptographic digests are committed to the audit layer; private data scopes or consortium subnets restrict cross-party visibility.
- Eventing and Provenance: The system emits signed, timestamped events (approvals, consents, revocations, shares, re-consent triggers) with immutable references (e.g., block height).
- Fault Tolerance and Idempotency: Audit commits employ retries with backoff; state-changing calls are idempotent; compensating actions unwind partial failures.

- Verification and Benchmarking: Property-based tests generate random state sequences to demonstrate invariants cannot be violated; differential tests ensure audit predicates match the formal logic. Security and privacy checks verify role scoping, private scopes, encryption at rest/in transit and revocation paths; performance benchmarks measure throughput and latency.
- Application Integration: Audit truth is wired to the UI state machine, so controls enable or disable based on committed state; human-readable receipts (e.g., "View approval receipt") promote transparency for non-experts.

## 7.5 Integration Plan

The integration plan is staged. First, the schema and chaincode definition translate the conceptual governance model into Fabric chaincode and SQL schemas. Second, an API layer provides secure RESTFull endpoints for consent lifecycle transitions, employing OAuth 2.0 and JWT. Third, front-end implementation builds Angular components for study pages, consent viewers, participant dashboards and IRB review modules. Fourth, DevSecOps incorporates automated CI/CD workflows using Docker, Azure Container Registry and AKS, with automated security scans. Finally, governance evidence is generated as cryptographically verifiable consent hashes and policy digests, accessible via a read-only peer. This architecture maps normative governance principles onto a robust technological stack, enabling a tangible, operational system for digital data governance (Drutskoy et al., 2013; Falessi et al., 2010; Henning, 2007; Miranda et al., 2023).

## 7.6 Actor Alignment

This one-to-one mapping demonstrates that no governance stakeholder is "left outside" the software boundary: every role that carries accountability in the framework is explicitly realized as a UML (Selic, 1998), actor with at least one compulsory interaction.

*Table 9 - Actor alignment table.*

| Governance Actor (Section 6) | UML Primary Actor | Rationale for Equivalence |
|---|---|---|
| Data Subject (personal-data sovereignty) | Participant | Owns the Grant / Revoke Consent and Access My Data History use cases, reflecting the right to control, audit, and erase PHI. |
| Public Health Researcher | Researcher | Initiates Create Study, Issue Re-Consent and Query Participant Status—functions that must be logged and endorsed on-chain. |
| Principal Investigator | PI (extends Researcher) | Adds Approve Study Protocol and inherits all researcher capabilities, modelling the hierarchical decision authority captured in the framework's structural mechanisms. |
| Institutional Review Board (IRB) | IRB Auditor | Sole owner of Approve Dynamic Consent Form; participates in Audit Ledger to enforce regulatory conformity. |
| Data Custodian / Private Company | Custodian API (external actor) | Consumes the Validate Current Consent and Push PHI Payload use cases before data transfer—an implementation of the framework's procedural gate-keeping rule. |
| Governance Committee (IODG) | System Governance Service | Supervises configuration of endorsement policies and channel membership through Update Network Governance; modelled as a secondary actor interacting with administrative use cases. |

## 7.7 Core Use Cases and their Governance Obligations

This section specifies the platform's core use cases and the governance obligations that constrain them. Building on Section 6's framework and the Methods in Sections 8 and 9, each use case is treated as a contract among stakeholders, participants, researchers, principal investigators (PIs), IRBs/auditors, and verified third parties, where roles, decision rights, and duties are translated into preconditions, postconditions, and enforceable controls. For every operational flow (e.g., creating or publishing a study; starting, pausing, or ending data collection; obtaining consent, re-consent, or withdrawal; and preparing data for sharing), we articulate the minimum approvals required, the consent status and privacy safeguards in force, the audit and provenance requirements (including optional ledger receipts), and the least-privilege access rules that must hold at every step. A complete use-case diagram and its descriptions are provided in Appendix B.

## 7.8 Governance-to-Implementation Traceability Matrix

This section presents the traceability matrix that links Section 6's governance requirements to the concrete design, implementation, and verification artifacts developed in Section 7. The matrix is the spine that runs through the section : each governance claim is mapped to (i) a precise software requirement, (ii) one or more design artefacts (use-case, class, and state diagrams; propositional-logic rules), (iii) the Consentio implementation component(s) that satisfy it, and (iv) the verification/acceptance activities that prove conformance. This makes the policy-to-platform pathway explicit, reviewable, and auditable.

### 7.8.1 Purpose and Scope

The traceability matrix has four complementary purposes within this thesis. It is first used to demonstrate completeness, showing that every governance directive articulated earlier is implemented in the Consentio platform rather than remaining at the level of policy intent. It also supports unambiguity by linking narrative requirements to formal, machine-checkable constraints, as defined in the logic formalization, and to concrete enforcement points in the platform's UI and API interfaces. In addition, the matrix strengthens testability by stating how each requirement is verified in practice, whether through unit or property-based tests, CI gates, audit queries, or usability checks. Finally, it enables auditability by identifying where immutable records are produced, such as approvals and consent changes, and by specifying how these records can be retrieved and analysed to substantiate compliance over time.

### 7.8.2 How to Read the Matrix

Each row corresponds to a single governance requirement originating in Section 6 and provides a structured chain from source directive to implementation evidence. The row begins with a stable requirement identifier used for consistent cross-referencing (for example, C1-GOV-10), followed by a brief paraphrase of the original governance source. It then states the derived requirement in Section 7 terms, describing the specific platform behaviour implied by the directive. The row next maps that requirement to the relevant design artefacts in Section 7, indicating where the rule is encoded, including the use-case diagram for stakeholder

interactions, the class diagram for the entities and associations carrying the constraint, the state diagram for lifecycle states and guarded transitions, the propositional logic that formalizes the invariant or guard, and the interfaces where the rule is enforced at the point of use. The row then identifies the Consentio implementation component responsible for satisfying the requirement and concludes with the verification or acceptance evidence that demonstrates compliance, such as tests, audits, or evaluation outcomes.

### 7.8.3 Traceability Matrix Table

The full traceability matrix is retained as an implementation artifact because it documents how governance commitments were translated into enforceable platform behaviour. The key reading is that each governance obligation is carried through four layers: the design requirement, the software component, the runtime check, and the verification evidence. This preserves reproducibility while keeping the chapter's main explanation focused on the governance-to-platform pathway. The complete traceability matrix is included as Table 10 in Appendix F.

### 7.8.4 Using The Matrix During Review and Implementation

To extend or use the traceability matrix during reviews, treat each feature as a row that must carry all five mappings: use-case, class, state, logic, and interface. During design review, verify that these mappings exist; any gap flags design debt to be resolved before implementation. In engineering, work from the Design Artifact Mapping as a running to-do list for guards, validators, and services, and reference the Req ID consistently in code comments and test names so the implementation stays tethered to its requirement.

For verification, convert the matrix’s Verification/Acceptance cell into concrete test plans: property-based tests for invariants, UI end-to-end tests for blocked flows, and audit assertions. In audits and compliance checks, use the same Req ID as the pivot to fetch ledger or audit evidence from the relevant endpoints and logs, ensuring a direct, reproducible link from requirement to proof.

#### 7.8.4.1 Using and Maintaining the Traceability Matrix

The traceability matrix functions as the practical control surface for review, implementation, and change control. During design review, each feature should be represented as a row that links the requirement to all core artifact types (use-case, class, state, logic, and interface); any missing link is treated as design debt and resolved before implementation. During engineering, the artifact mapping becomes the implementation checklist for guards, validators, and services, and the requirement identifier should be carried consistently into code comments and test names so the build remains anchored to the originating governance directive. Verification then follows directly by turning the matrix's acceptance criteria into executable evidence, including tests for invariants and blocked flows as well as audit assertions, while audits and compliance checks use the same requirement identifier to retrieve ledger or log evidence through the relevant endpoints. Because governance policies and actor configurations evolve, the matrix is maintained as a versioned artifact: when a directive changes or a new process is added, the derived requirement, mappings, impacted components, and acceptance evidence are updated together, and the revision history is preserved through explicit version increments and recorded diffs. In parallel, the class model provides the platform vocabulary that these rows constrain and operationalize, covering study lifecycle and oversight (Study and its companion structures), review roles and approvals, dynamic consent structures and immutable records, communication and accountability surfaces, contextual instrumentation, privacy-preserving reporting, and policy gating through endorsements, which together form the domain substrate for the subsequent state, logic, and interface enforcement.

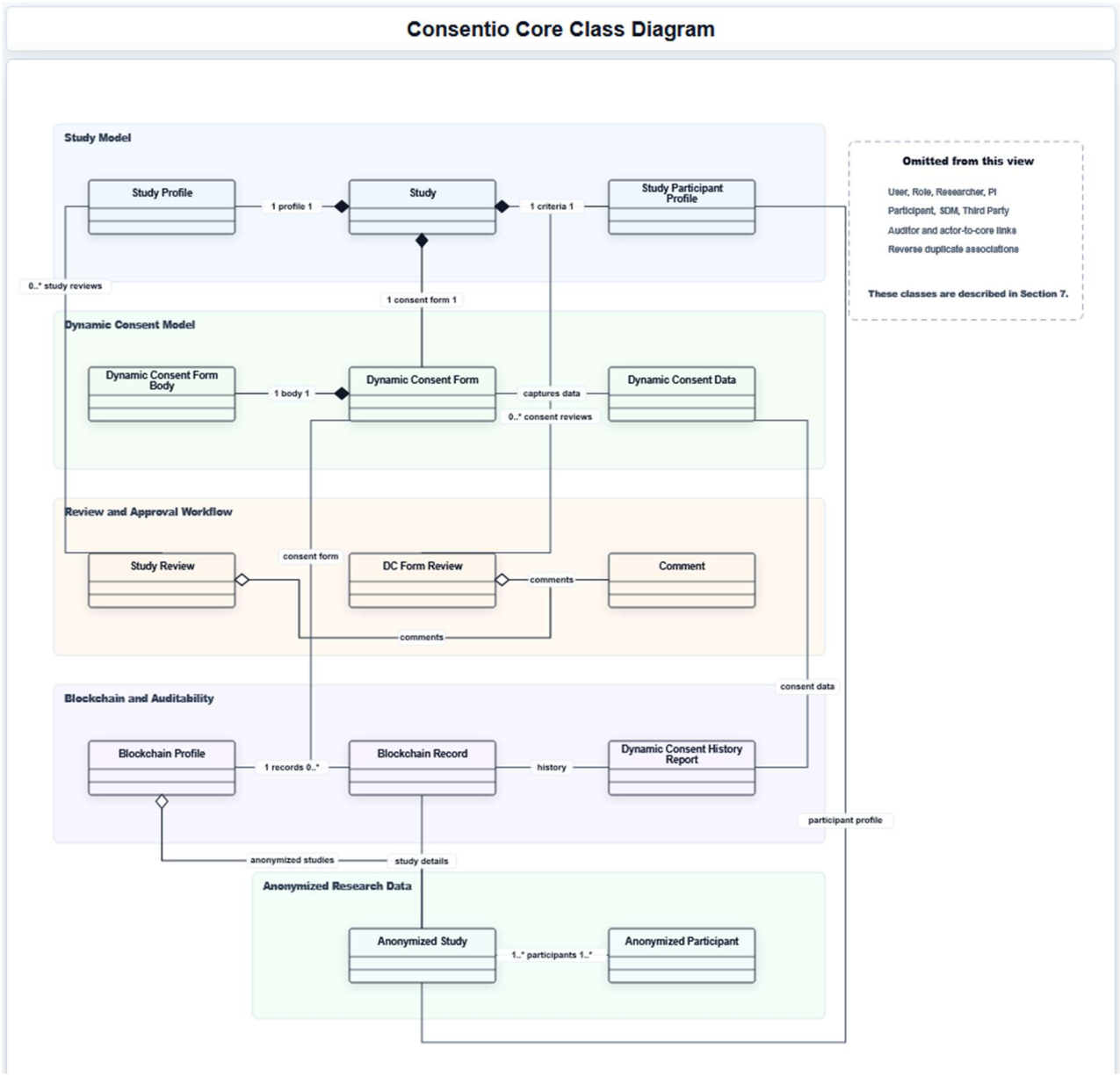
## 7.9 Consentio Platform's Class Diagram

The static view of Consentio is captured in the "*Consentio Platform Class Diagram*" (see Figure 7). Every rectangle in the diagram embodies one conceptual class that lives in the domain layer, and each of them traces directly to (i) an actor/artifact surfaced by Section 6's Governance Framework, or (ii) an infrastructure object required to implement the framework's control, audit-trail and communication

mechanisms. The model is deliberately split into five logical aggregates (Figure 7) to preserve bounded–context cohesion and to mirror the governance responsibilities allocated in the GAF mapping.

The class diagram is retained as a reference architecture rather than as the primary explanation of Consentio. The main point for the reader is that the platform entities mirror governance obligations: studies carry approval and lifecycle states, consent forms carry versioned permissions, participant actions create consent transactions, and audit records preserve evidence of material state changes.

*Figure 7 - Platform class diagram.*



The GAF mapping aggregate can be found below at Table 10.

*Table 10 - GAF Mapping.*

| Aggregate | Governance Facet |
|---|---|
| Identity & Access | Role–segregation, authentication, invitations |
| Research Lifecycle | PI/Researcher authoring, IRB review, study status work-flow |
| Dynamic Consent | Data–subject sovereignty, blockchain traceability |
| Communication | Auditable researcher–participant dialogue |
| Anonymized Analytics | Public-health secondary analysis at low re-identification risk |

A detailed description of each class in the diagram is presented in Appendix C.

## 7.10 State Diagrams and Governance Alignment

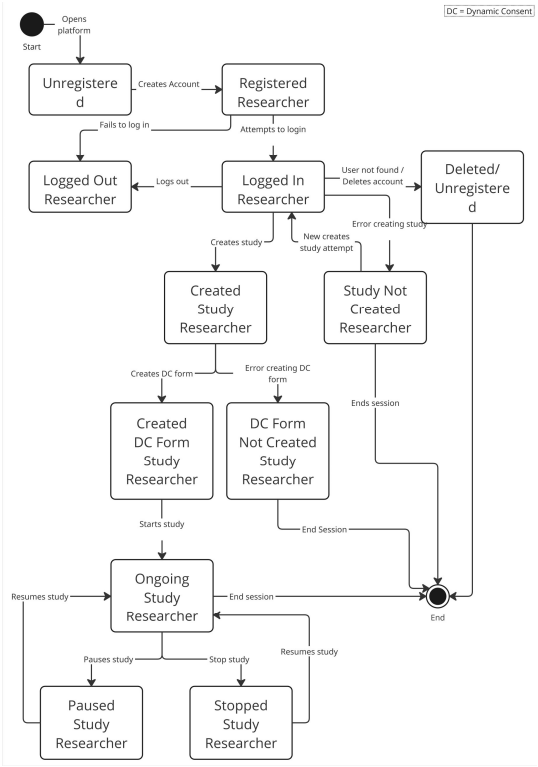
The state diagrams are included to document lifecycle constraints, but their central purpose is straightforward: no study, consent form, approval decision, or participant action should move into a state that violates the governance model. The chapter therefore summarizes the practical meaning of each lifecycle before presenting the detailed diagram.

Consentio operationalizes dynamic consent through actor-specific state diagrams and study state diagrams (Lange et al., 2006; Oldevik & Berre, 1998) that define how studies and consent transactions move from creation to approval, execution, pause, and closure. The diagrams allocate responsibilities across researchers, auditors, participants, and principal investigators (PIs), and embed governance principles from Section 6 by making key actions conditional, reviewable, and auditable. In doing so, the workflows enact respect for persons, beneficence, and justice as articulated in the Belmont Report (Hiroko Nagai et al., 2022; Sims, 2010), the voluntary consent requirements of the Nuremberg Code (Cosman, 2023), and the broader ethical obligations of the Declaration of Helsinki (Association, 2013). Governance is implemented through participant control, transparent accountability, and role-based permissions, supported by dynamic consent mechanisms and immutable audit trails.

### 7.10.1 Researcher State Diagram

The researcher's state diagram (Figure 8) describes the progression from registration and authentication to study creation, consent-form drafting, and study operations. Authentication gates entry into study functions and failed actions (for example, unsuccessful creation of a study or consent form) keep the researcher in corrective states until errors are resolved, ensuring accountability through explicit checkpoints. Once a study is ongoing, the researcher can pause, resume, or stop it, with logout and account deletion terminating access to prevent unverified or unauthorized management of studies. Overall, the diagram enforces a sequenced workflow in which study creation, consent preparation, and execution occur in a controlled order that reduces accidental violations of participant rights.

*Figure 8 - Researcher State Diagram.*




#### 7.10.1.1 Alignment with Governance Framework

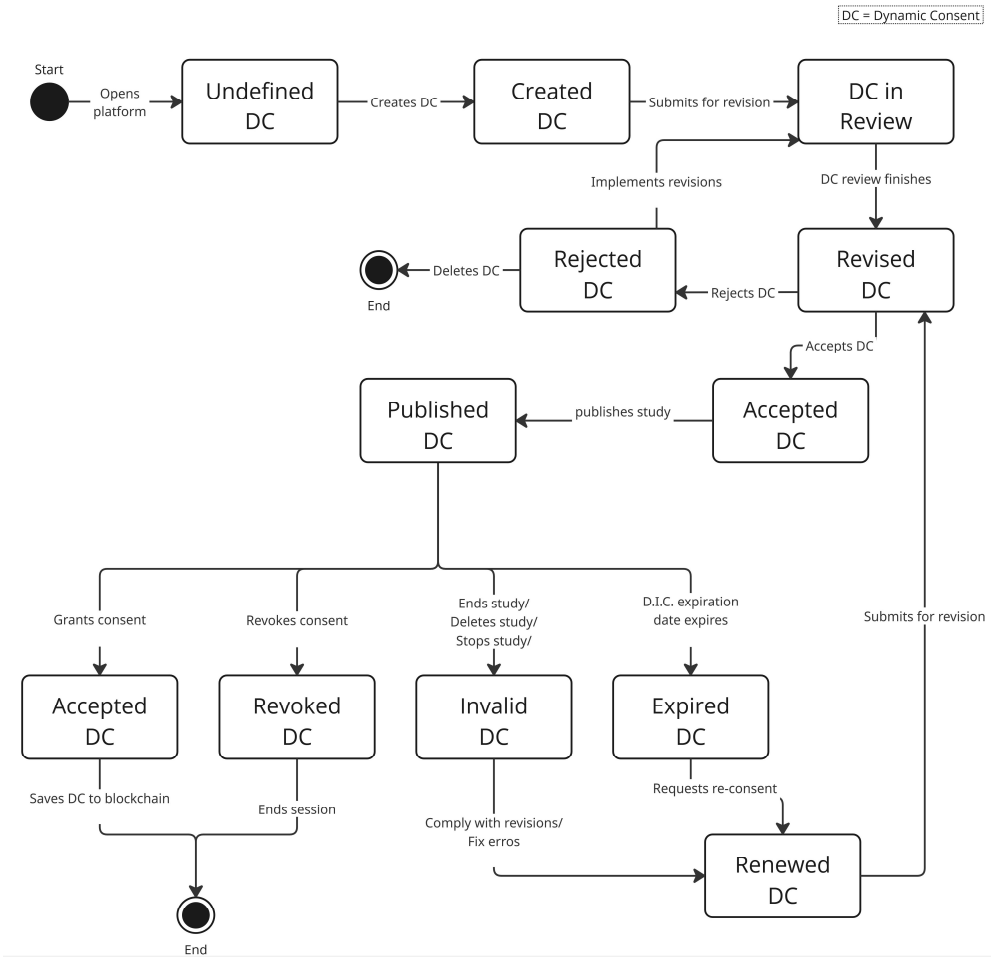
The researcher state flow operationalizes consent governance by requiring explicit approval at each step. It adheres to the principle of respect for autonomy by ensuring that no study proceeds without a valid informed

consent form. Errors in study or consent form creation prompt the researcher to correct the problem before the study can be started, protecting participants from misconfigured consent requests. The ability to pause or stop a study supports beneficence and non-maleficence: if new risks or technical issues are identified, the researcher can halt recruitment or data collection to reassess. Moreover, the system logs all transitions, contributing to an immutable audit trail that meets the transparency requirement.

### 7.10.2 Dynamic Informed Consent (DC) Form State Diagram

The dynamic consent form state diagram (Figure 9) compresses the consent lifecycle into a governed pipeline, from drafting through publication to post-publication participant control. The form progresses from an initially undefined state to a created state, then enters review upon submission, where the auditor and PI assess whether it is rejected for revision or accepted for publication alongside the study. Once published, the form is not merely static; it becomes an operational object whose state reflects participant decisions, including acceptance recorded on the blockchain and revocation, which ends authorization for participation. The diagram also captures time and lifecycle constraints through invalidation at study termination and expiration for time-bounded consent, with renewal supporting periodic re-consent in long-term studies. Importantly, any post-publication modification is routed back through the same review gates, preserving the requirement that consent remains informed, valid, and subject to oversight.

*Figure 9 - Dynamic Informed Consent Form State Diagram.*



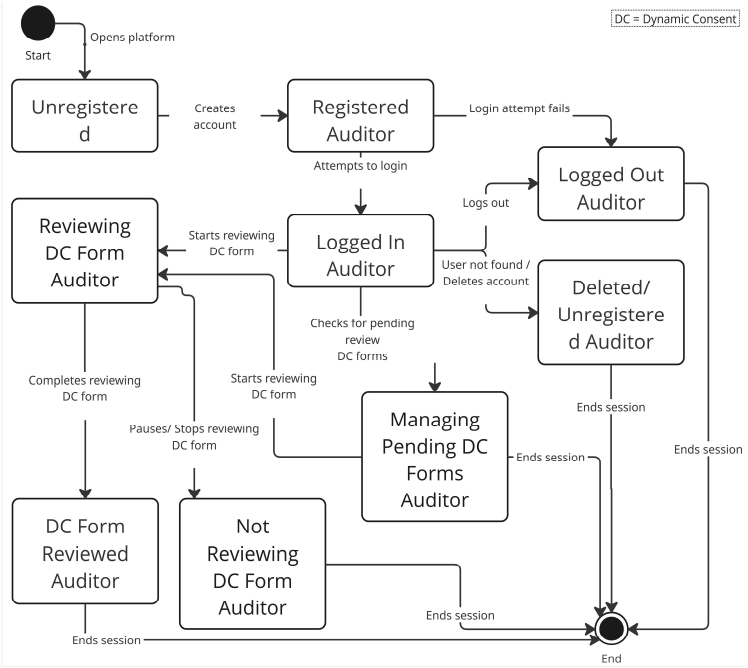

### 7.10.2.1 Addressing Consent Challenges

Dynamic consent addresses the limitations of traditional consent by formalizing renewal and revocation procedures, ensuring that withdrawal is always possible and operationally enforceable. The explicit revocation state aligns with the voluntary participation requirements of the Nuremberg Code, while expiration and renewal support sustained communication in long-running studies. Separate approvals by auditors and PIs add safeguards against coercion and misalignment with ethical and legal requirements. Logging final consent states on a blockchain strengthens transparency by providing a tamper-resistant record of what was consented to and when (Assale et al., 2019; Budin-Ljøsne et al., 2017; Musmade et al., 2013; Politou et al., 2018; Rothwell et al., 2021).

### 7.10.3 Auditor State Diagram

The auditor state diagram (Figure 10) models independent review of dynamic consent forms, from registration and login to managing pending forms and conducting reviews. Auditors transition between pending management and active reviewing, and the workflow permits pausing without allowing unreviewed forms to advance. Review actions, including comments and decisions, are logged to create an evidentiary trail. Logout and account deletion remain possible, but do not bypass the requirement that only authenticated auditors can issue approval or rejection decisions.

*Figure 10 - Auditor State Diagram.*



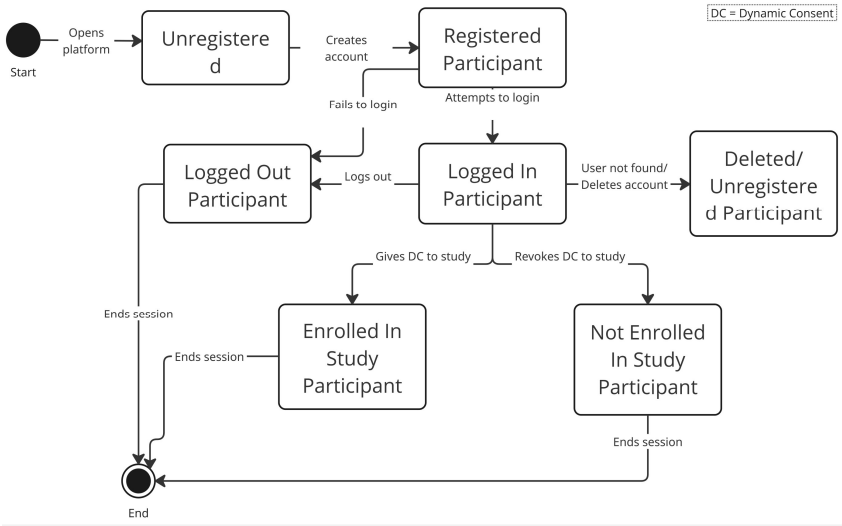

#### 7.10.3.1 Compliance and Independence

Separating auditor workflows from those of researchers and PIs enforces independence and reduces conflicts of interest. By requiring completion of review steps before consent forms can be published, the design instantiates oversight expectations analogous to post-Belmont institutional review mechanisms. The pause-and-resume capability supports careful review without allowing silent progression, preserving the integrity of governance checks while remaining practical.

### 7.10.4 Participant State Diagram

The participant state diagram (Figure 11) focuses on a minimal set of actions: register, authenticate, view studies, consent, and revoke. Participants can move between enrolled and not enrolled states through explicit consent decisions, and withdrawal immediately updates participation status and associated access permissions, preserving voluntariness and revocability as required by the Nuremberg Code (Cosman, 2023). The simplified flow reduces cognitive burden and supports autonomy, while secure authentication and blockchain-backed records provide participants with clearer evidence that their choices were recorded and acted upon.

*Figure 11 - Participant State Diagram.*




#### 7.10.4.1 Respecting Autonomy and Privacy

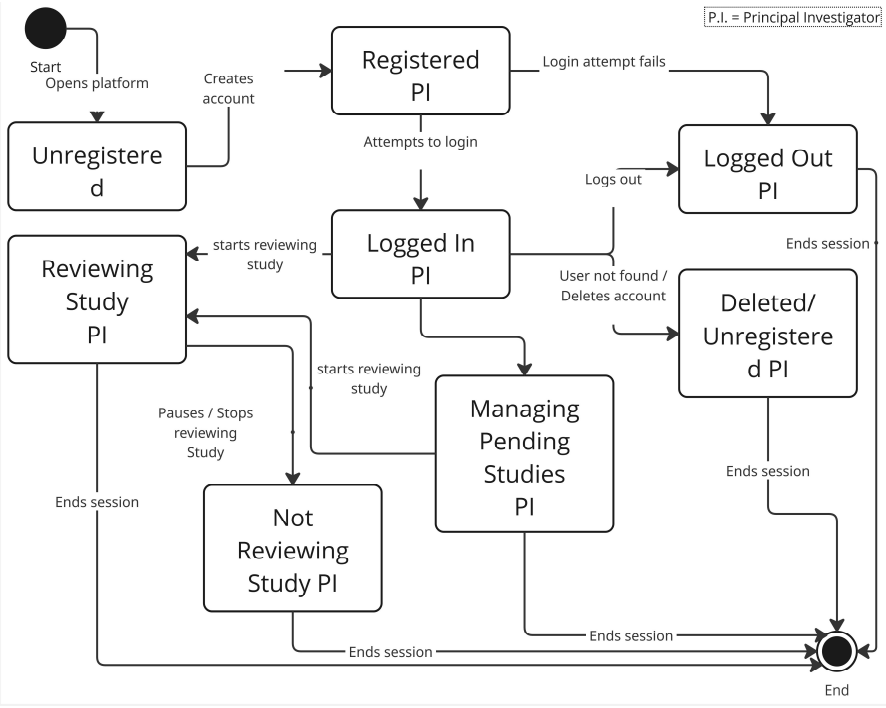
The participant flow is essential to upholding the ethical principle of respect for people. Participants can manage their consent decisions at any time, and the system immediately updates the study's roster and associated data access permissions. This ensures that participation is always voluntary and revocable. By simplifying the process, the platform mitigates cognitive burdens and reduces the risk that individuals inadvertently remain in a study they no longer wish to participate in. Secure authentication protects

participant data in compliance with privacy regulations. The direct link between participant actions and blockchain records provides participants with reassurance that their choices are recorded transparently.

### 7.10.5 Principal Investigator (PI) State Diagram

The PI state diagram (Figure 12) captures oversight as a distinct workflow in which PIs manage pending studies, initiate reviews, pause when needed, and conclude with approval or rejection. Approval routes the study toward publication within the study lifecycle, while rejection returns it to the researcher for revision. The separation of PI actions from researcher actions creates a traceable chain of responsibility for study release decisions, strengthened by logged transitions that support accountability.

*Figure 12 - Principal Investigator (PI) State Diagram.*




#### 7.10.5.1 Oversight and Accountability

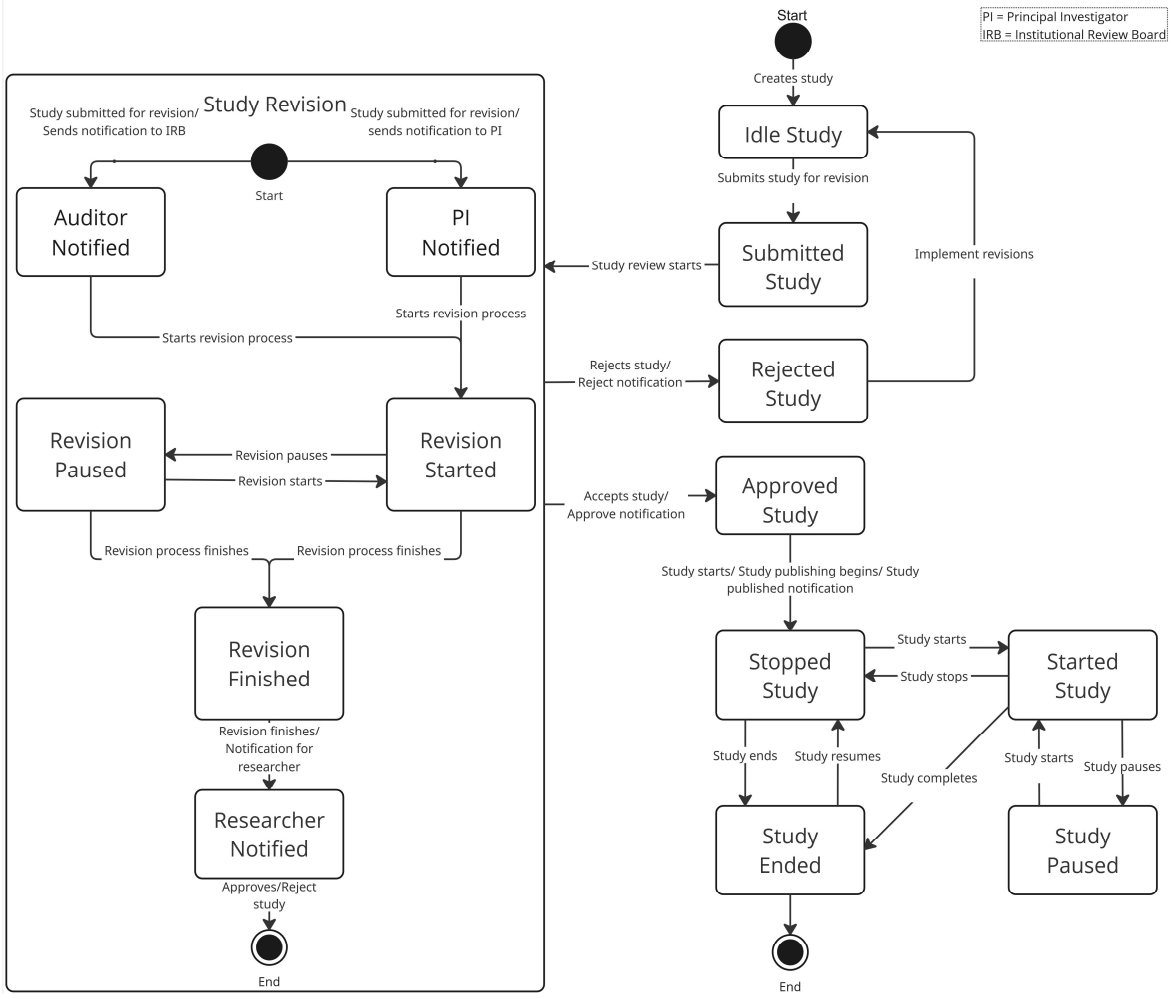
The PI's role acts as the final gatekeeper before a study is publicly available. The separate PI state diagram underscores the governance principle of separation of duties: researchers cannot unilaterally publish studies; they require PI and auditor approval. This reduces the likelihood that unethical studies will progress

unchecked. The ability to pause reviews acknowledges that complex studies may require additional consultation or risk assessment. Each state transition is logged into the blockchain, providing evidence of due diligence and compliance.

### 7.10.6 Study Approval State Diagram

The study approval flow (Figure 13) begins after study creation. It moves through submission, independent review by the IRB and PI, and a revision loop that continues until both approvals are obtained. When both reviewers approve, the study transitions to an approved state and, where enabled, is registered on a ledger to create an immutable record of the approved protocol and consent artifacts before recruitment begins. Registration failures trigger retries, after which a fail-safe termination state is entered to prevent silent progression without auditability. Once registered, the study enters a published but inactive state for readiness, then transitions to started when recruitment and data collection commence. Study execution is coupled to the consent-form lifecycle so that starting enables consent capture, pausing or stopping halts collection under the current authorization, and meaningful changes can trigger re-consent to preserve the temporal relevance of consent.

*Figure 13 - Study Approval State Diagram.*




### 7.10.6.1 Governance Implications

The flow operationalizes dual oversight (IRB and PI) and immutable record-keeping. Requiring both approvals prior to publication, and, where enabled, ledger registration before any start, creates a clear, auditable chain from review decisions to operational states. The retry-with-fail-safe pattern prevents progression when critical audit steps cannot be recorded, avoiding silent non-compliance. Overall, the model ensures that no study can start without appropriate approvals, that pauses and stops are explicit and recoverable, and that end-of-study actions (including consent invalidation and data handling) are deterministic and reviewable, reinforcing ethical principles (beneficence, respect for persons, justice) and regulatory expectations for transparency and reproducibility.

### 7.10.7 State Diagrams Summary and Informed Consent Challenges

Together, the diagrams turn governance commitments into enforceable pathways: consent remains voluntary and revocable through explicit renewal and revocation states (Cocanour, 2017; Fatema et al., 2017; Musmade et al., 2013; Prictor et al., 2020; Resnik, 2009; Thompson & McNamee, 2017), Oversight is distributed through independent auditor and PI approvals, and accountability is supported by immutable records of critical transitions (Benchoufi et al., 2018). The ability to revise, pause, and resume studies supports responsiveness to emerging risks and evolving requirements, including contexts that demand rapid yet ethical data use, such as during the COVID-19 pandemic (Rothwell et al., 2021). At the participant level, the simplified enrollment and withdrawal flow aims to reduce accessibility barriers and mitigate disadvantages associated with lower digital literacy (Jurkovic & Kopal, 2025; Steelman et al., 2016). Simultaneously, the workflows make dynamic consent a lived, operational practice rather than a declarative policy, aligning inter-organizational sharing with participant control, accountability, and role-based permissions.

## 7.11 Formalized Logic and Constraints for Consentio

Dynamic consent is a paradigm in which participants control how and when their personal data are used in research. Traditional consent forms are static, offering only an up-front choice. Dynamic consent attempts to support ongoing preference management, granular permissions and transparency. To deliver these capabilities at scale, a platform must ensure that every operation satisfies legal and ethical rules. Therefore, this section introduces a formal specification of Consentio, the proposed dynamic-consent platform. The formalization draws on propositional logic and, where necessary, first-order logic to encode the states and transitions of studies, participants and consent transactions. Propositional logic treats statements as atomic propositions—truth values that can be combined with logical connectives such as conjunction (∧), disjunction (∨), negation (¬) and implication (→). When these propositions are attached to well-defined system states—such as a study being *ongoing* (So), *paused* (Sp) or *ended* (Se)—logic provides a precise language for expressing which actions are allowed at any time. For example, the invariant $So \rightarrow (Ia \wedge Pa)$

states that a study can be ongoing only if both institutional-review-board and principal-investigator approvals are true. First-order logic is employed only when quantification over participants, studies or transactions is essential, for instance, to assert that every enrolled participant must have previously been invited.

The section argues that prose descriptions of governance rules are insufficient for automated enforcement. A formal specification translates obligations, such as "share data only with current consent", into invariants like $Dshare \rightarrow (Pg \wedge \neg Pr)$ that can be checked by the platform's smart contracts and validators. The choice of propositional (and propositional dynamic) logic is well aligned with system design: modal logics can represent states and events of dynamic systems and reason about both computation states and the transitions between (Troquard & Balbiani, 2007). In Propositional Dynamic Logic (PDL), statements describe what must be true after a program's executionplato.stanford.edu, making it a natural fit for expressing conditions that must hold before and after user actions. By grounding the platform's behaviour in these logics, Consentio gains a rigorous, machine-checkable specification that underpins trust and auditability.

Section 25, therefore, introduces the basic notation used throughout the thesis. Atomic propositions are defined for study lifecycles, approvals, participant states, consent transactions and privacy settings. Connectives enable the composition of these propositions into invariants and guards. The section explains how conjunctions enforce simultaneous conditions, disjunctions express alternatives, negations prohibit unwanted states, and implications encode preconditions. The use of equivalence (↔) captures bidirectional relationships such as "a study is paused if and only if data collection is stopped and recruitment is closed." The formalism is complemented by selective quantifiers: ∀ expresses that a property holds for all participants or studies, while ∃ denotes the existence of an entity satisfying a condition.

The contribution of this formalization is threefold. First, it offers a methodological contribution, showing how governance principles can be converted into executable invariants for dynamic-consent systems. Second, it yields an empirical contribution by ensuring that recorded metrics, such as consent

latency, re-consent rates and withdrawal patterns, are measured within legally permissible state spaces. Third, it provides a practical contribution: an engineering blueprint that includes guards, validations, smart-contract predicates and monitoring components. These artifacts support reliable and auditable deployments and ensure that every action taken by a participant or researcher is justified by a corresponding logical rule. Limitations of the approach are acknowledged: propositional logic does not capture temporal ordering, and not all ethical considerations reduce neatly to logic. Nevertheless, within its scope, the formal specification greatly enhances clarity, verifiability and enforceability.

## 7.12 Entities and Propositional Variables

While propositional logic supplies the grammar for expressing invariants, it is the vocabulary of domain entities and variables that anchors those invariants in the real world. Section 26 delineates the semantic layer of Consentio by enumerating the core entities and their associated propositional variables. Each entity, such as Study, ParticipantStatus, Version, Invitation, ConsentTransaction, PrivacySettings, Feedback and Third-Party Data Use, serves as a locus of truth assignments over time. Variables attached to each entity are mainly Boolean, toggling on or off in response to lifecycle events. For example, the study entity defines mutually exclusive states Sn (new), Sd (draft), Spa (pending approval), So (ongoing), Sp (paused), Su (suspended) and Se (ended). Approval variables (Ia, Pa, Ra) distinguish institutional-review-board, principal-investigator and regulatory decisions. Participant-flow variables—Pi (invited), Pe (enrolled) and Pw (withdrawn)—capture the participant lifecycle, while consent-transaction variables—CTe (enrolled), CTw (withdrawn), CTp (pending) and CTr (rejected)—encode the state of an individual consent record.

Not all variables are Boolean; some represent counters or scalar scores. For instance, CPIQ variables capture user feedback on clarity, privacy, interface and quality; V_cnt, W_cnt, L_cnt and E_cnt track page views, wish-lists, logins and enrolments. Others, such as Sv, hold version identifiers as non-empty strings. Naming conventions use short mnemonics and suffixes to maintain readability. The suffix _ST_SLEEP binds a predicate to the Sleep study example used later; _P_ANA and _U_PI bind predicates to specific participants or user roles (e.g., principal investigator). These conventions enable variables to be

reused across entities without ambiguity. Table 5 in the original thesis (Logic notation table) summarizes the notation for suffixes, lifecycle states, approvals, operational gates, versioning, participant flow, consent transactions, privacy and sharing flags, outcomes, feedback metrics, counters and role capabilities. For completeness and to facilitate replication, the details of each variable and its domain are provided in Appendix D.

*Table 11 - Propositional logic variables and meaning.*

| Symbol / Suffix | Meaning | Example |
|---|---|---|
| _ST_SLEEP | Binds a predicate to the Sleep study instance | *So_ST_SLEEP = "the Sleep study is 'ongoing'"* |
| _P_ANA, _P_BEN | Participant-scoped predicates for "ANA," "BEN" | *Pe_P_ANA = "ANA is 'enrolled'."* |
| _U_ANA, _U_PI, _U_IRB, _U_TP | User-scoped predicates (participant, PI, IRB, third-party) | *Rc_U_PI = "PI user can 'create' a study"* |
| Lifecycle | Sn "*new*", Sd "*draft*", Spa "*pending approval*", So "*ongoing*", Sp "*paused*", Su "*suspended*", Se "*ended*" | — |
| Approvals | Overall/IRB/PI triplets: A*, I*, P* with p "*pending*", a "*approved*", r "*rejected*" | *Ia* = "*IRB 'approved'"* |
| Ops gates | Ro "*recruitment open*", Do "*data collection on*", Ds "*data collection stopped*" | — |
| Versioning | Sv "*current version id*" (non-empty) | — |
| Participant flow | Pi "*invited*", Pe "*enrolled*", Pw "*withdrawn*" | — |
| Consent tx | CTe "*enrolled*", CTw "*withdrawn*", CTp "*pending*", CTr "*rejected*" (per transaction) | — |
| Privacy & sharing | Da "*anonymized*", Dn "*not anonymized*", Dshare "*share action*", Pg "*consent granted*", Pr "*consent revoked*" | — |
| Outcomes | Oo "*outcome observation on*", On "*off*" | — |
| Feedback | Fr "*rating*" (0–5), Fc "*comment*" | — |
| CPIQ | CS "*score*" (≥0), PB "*public-benefit text*", SB "*study-benefit text*" | — |
| Counters | V_cnt "*views*", W_cnt "*wishlists*", I_cnt "*invites*", L_cnt "*logins*", E_cnt "*enrollments*" | — |
| Capabilities | Rc "*researcher create*", Rs "*researcher submit*", Rm "*researcher manage participants*", PIr "*PI approve/reject*", IRBr "*IRB approve/reject*", TPc "*third-party checks*" | — |

By defining a canonical state vocabulary, Section 7 ensures that later constraints and invariants have an unambiguous domain of discourse. Logical claims map directly to executable system behaviour because each proposition corresponds to a database field, a smart-contract variable or a user-interface flag. The careful typology of variables, Boolean, enumerated, or numeric, also allows static type checking and domain restrictions to be expressed formally.

## 7.13 Constraints by Entity

The heart of the formal model lies in the constraints that bind variables into admissible combinations. Section 7 systematically enumerates safety properties, progress obligations and domain restrictions for each entity. Safety properties specify conditions that must never occur ("nothing bad happens"), progress obligations guarantee liveness ("something good eventually happens"), and domain restrictions ensure well-formedness (e.g., mutual exclusivity of statuses, non-emptiness of required fields, non-negativity of counters). These properties collectively prevent ethically or legally impermissible configurations from becoming reachable and ensure that the research lifecycle advances only when clearly articulated preconditions are met.

For the StudyEntity, the logic asserts that a study can be ongoing only if both IRB and PI approvals are granted ($So \rightarrow Ia \wedge Pa$), that recruitment can open only in the draft state with approvals in place, and that data collection cannot start unless recruitment has occurred. Transition constraints forbid illegal jumps: a study cannot move directly from new to paused or ended; suspending or resuming a study is only meaningful if the study was previously ongoing and has not already ended. Version governance is formalized by requiring a non-empty version identifier ($Sv \neq \emptyset$) and stipulating that activating a new version presupposes approvals from both IRB and PI. This ensures that participants always consent to an explicitly approved version of the protocol.

In the ParticipantStatusEntity, enrolment (Pe) is permitted only after invitation (Pi) and cannot persist after withdrawal (Pw). Withdrawal implies that a participant's data collection and sharing must stop ($Pw \rightarrow \neg Ro \wedge \neg Do$), while re-consenting is possible only if a new version has been activated and both approvals are still valid. The InvitationEntity enforces that invitations are sent only when the study is approved, that each email is valid and unique, and that invitations expire if the study transitions to a state where recruitment is closed. The ConsentTransactionEntity specifies that a consent record begins in a pending state, can be completed or rejected, and can be withdrawn only after it has been granted. Withdrawals trigger revocation of data sharing and anonymization flags.

The ThirdPartyDataUseEntity deals with privacy and data-use permissions. Sharing data with third parties is allowed only when consent has been granted (Dshare → Pg ∧ ¬Pr) and when anonymization is consistent with the participant's choice. External processing is prohibited when consent is revoked or absent. Suspension/resumption semantics refine lifecycle transitions: suspension is only coherent for ongoing studies, and resumption requires a prior suspension event. These semantics are encoded as guards on transition events rather than global assertions; the platform enforces them at the point where an operation attempts to change state, preserving both soundness and usability.

Other entities carry their own constraints. For VersionEntity, version identifiers cannot be empty, and only one version is active at a time. The FeedbackEntity requires ratings to fall between 0 and 5 and mandates that each comment be associated with a valid participant and study. Counters such as login counts, view counts and wish-lists must be non-negative. The UserInteractionEntity stipulates that every event—invites, enrolments, withdrawals, logins or views—is attributable to a valid user account. The NotificationEntity requires that notifications specify type, title, body, timestamp and icon. A ContactListEntity must exist for study communications, and a ProfileImageEntity is mandatory for user identification. Detailed information about the propositional logic modelling can be found in the Appendix D.

## 7.14 Operationalizing Consent Governance: Interfaces and Functionalities

Translating the formal model into software behaviour, the Consentio platform treats user interfaces not as cosmetic layers but as governance instruments. Every control and navigation path emerges from the atomic propositions and invariants defined in the formal framework. A comprehensive traceability matrix links each governance clause to a formal constraint, a user-interface affordance, an automated test, a stored procedure and a ledger-backed audit event. This bi-directional mapping, from normative principles to UI widgets and back to the rules that justify them, satisfies regulatory demands for accountability and traceability and ensures that each interaction is anchored to a verifiable rule.

The core workflow comprises drafting, approval and execution of studies. Principal investigators (PIs) register research protocols through a study management dashboard, entering descriptions, objectives, methodologies, inclusion criteria and data-collection instruments. Mandatory fields and version identifiers are enforced before the protocol can progress to approval. IRB members receive notifications and must approve or reject; conflicting approvals are prevented, and unanimous decisions are required when configured. Only after both IRB and PI approvals are granted does the study enter an "ongoing" state, enabling recruitment and data collection. Suspension and resumption controls enforce the transition guards defined in the formal model. A recruitment interface manages invitations: investigators input email addresses, which the system validates; personalized tokens embed dynamic consent links; and re-invitation is prohibited until previous invitations expire or protocols change. Each invitation generates a ledger entry and an email notification.

Consent collection uses a dynamic form reflecting the approved study version. Participants review study information, select data-collection options, set sharing and anonymization preferences and indicate whether they wish to receive results. They cannot submit until mandatory fields are acknowledged, and eligibility issues are displayed. Submission creates a pending consent transaction ($CT_p$); investigators countersign to complete the transaction ($CT_e$). Participants access a consent history page listing versions, statuses (granted or withdrawn), timestamps and blockchain hashes for independent verification (Appenzeller et al., 2022; Budin-Ljøsne et al., 2017; Dankar et al., 2020). A participant management panel allows investigators to monitor enrolments and manage withdrawals: when a participant withdraws, data collection and sharing cease automatically, and metrics update. A version manager supports protocol amendments; new versions require IRB and PI approval and trigger re-consent cycles. A secure chat replaces ad-hoc email exchanges, logging all communications for audit.

To support analysis and continuous improvement, a historical dashboard displays metrics such as consent latency, re-consent rates, withdrawal rates, login counts and feedback scores. These metrics derive from formal variables and are meaningful because the platform guarantees that all interactions conform to

the governance rules. A chat simulator trains administrators by presenting scenarios and logging decisions. Crucially, every UI action triggers an auditable, time-stamped record anchored on a private ledger, ensuring immutability and accountability. Controls are disabled unless preconditions are met; attempted violations return explanatory messages referencing the relevant rule, guiding users through compliant workflows. Figure 14 below illustrates some of the developed interfaces.

The interface workflow is best read as two connected user journeys rather than as a collection of isolated screens. The first journey represents the participant experience, while the second represents the researcher and administrator experience. Together, these workflows show how Consentio translates governance requirements into visible platform actions.

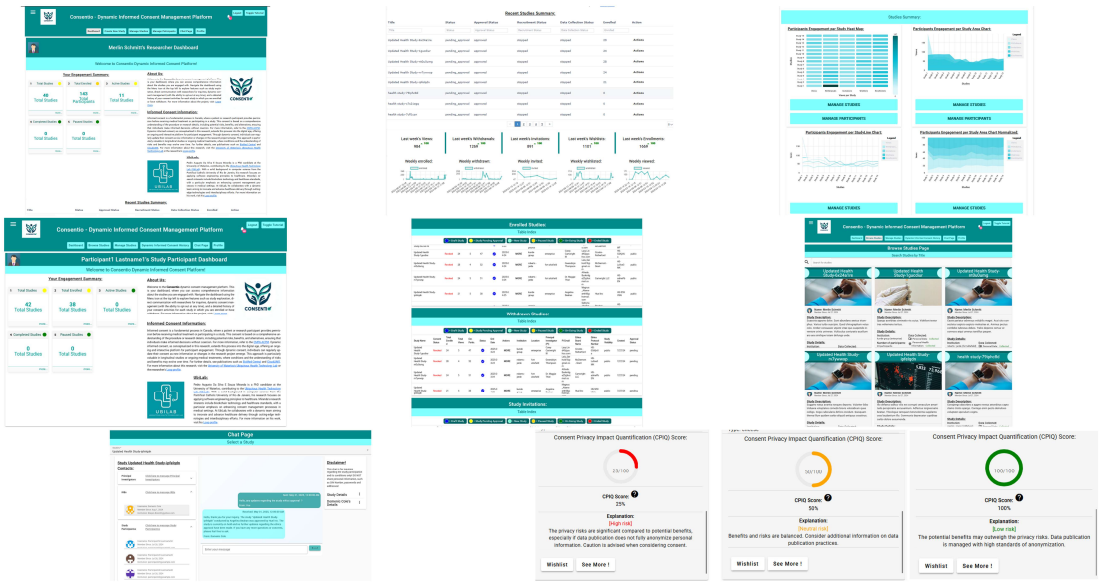
For participants, the workflow begins with study discovery. A participant can browse available public health studies, review study summaries, and access layered information about the study purpose, data collection methods, risks, benefits, and privacy expectations. The next step is consent review, where the participant reads the dynamic informed consent form and examines the specific permissions being requested. After reviewing the information, the participant may grant consent, adjust permission preferences, or decline participation. If consent is granted, the platform records the decision as a consent transaction and makes the participant's consent status visible in their dashboard. The participant can later return to the platform to review their consent history, verify ledger-backed receipts, modify preferences when allowed, or withdraw consent. Withdrawal is treated as a governance-relevant action because it updates the participant's study status, changes data access permissions, and creates an auditable record of the decision.

For researchers and administrators, the workflow begins with protocol setup. Researchers create or configure a study, define study metadata, prepare the dynamic consent form, and submit the study for the required review process. The platform then supports approval tracking by making the status of PI and IRB review visible before the study can move forward. Once the study is approved and published, researchers can invite participants, monitor enrollment, view consent states, and identify participants who may require

re-consent after a protocol or consent-form change. The workflow also includes participant communication through notifications and messaging, allowing researchers to send updates, answer questions, and manage study-related interactions in a more centralized way. Finally, researchers and administrators can access audit and reporting functions, which provide evidence of approvals, consent grants, withdrawals, re-consent events, and other material state changes.

This step-by-step workflow is important because it shows that Consentio's interfaces are not only usability features. Each visible action corresponds to a governance rule or system constraint. A study cannot proceed without the required approvals, consent cannot be recorded without participant action, withdrawal must update the participant's status, and key decisions generate auditable records. In this way, Figure 14 should be read as a walkthrough of how the platform operationalizes dynamic consent, participant control, researcher accountability, and ledger-supported auditability through connected interface actions. Appendix E contains all relevant interface images in higher resolution, accompanied by a brief description.

*Figure 14 - Consentio participant and researcher interface workflows.*



### 7.14.1 Participant Interfaces

For data subjects, Consentio provides a unified dashboard listing all studies in which they participate. Each entry shows consent status (active, revoked or pending), date, version and a blockchain verification hash. Dynamic controls allow participants to grant, update or revoke consent and adjust permissions per data type (e.g., wearable sensors, surveys, location data, genomic data). Preferences for receiving study results and contact modalities (email, telephone or messaging) are configurable. Layered information design helps participants understand research: concise summaries lead to expanded sections with full protocols and external resources; tooltips, guided tours and glossaries explain technical terms; and multimedia elements illustrate study rationales and data flows (MRCT Center, 2016). Two-way communication via the chat interface allows participants to ask questions and receive updates; notifications inform them when new consent forms are available or when study results are released.

Dynamic consent features overcome the limitations of broad one-time consent models by enabling granular choices and ongoing engagement. Real-time visibility into data use aligns with GDPR transparency requirements, and blockchain hashes reinforce trust by enabling participants to verify immutability of their consent records. Feedback mechanisms (rating scales and comment boxes) encourage participants to report their experiences, feeding into the historical dashboard for iterative improvement.

### 7.14.2 Researcher and Administrator Interfaces

For researchers and administrators, a management dashboard organizes studies by status and highlights actions required. A “create study” wizard guides investigators through defining objectives, methodologies, inclusion and exclusion criteria and ethics documentation, enforcing mandatory fields and cross-referencing entries against governance requirements. The wizard previews participant-facing consent forms, enabling researchers to refine wording for clarity and compliance. On submission, the system notifies IRB reviewers and tracks their decisions.

Within the participant management panel, researchers can view enrolled individuals, consent statuses and demographic breakdowns. An anonymized data-export function honours participants' anonymization preferences, and a re-consent manager lists those who must re-consent due to amendments. Personalized notifications encourage prompt re-consent, and statistics such as consent latency and withdrawal rates highlight studies requiring additional communication. The chat interface logs all communications with time stamps and identifiers, enforcing non-disclosure of personally identifiable information unless permitted.

### 7.14.3 Rationale and Evaluation

The interface design synthesizes human-computer interaction principles, clarity, consistency, feedback, and error prevention, with the governance model. Layered information respects cognitive load, letting users access more detail when needed; progress indicators show position in workflows; and explanatory messages reference underlying rules when actions are unavailable. These features promote agency, transparency and trust, core tenets of dynamic consent. A pilot evaluation reported that users valued consent tracking, centralized participation history and access to study results; immutable ledger records enhanced trust, although further explanation of blockchain was requested. Interface responsiveness and simplification for less technical users emerged as improvement areas, but overall willingness to participate in research was high. Continuous feedback, together with the formal model's flexibility, will guide future iterations, ensuring that Consentio remains a robust implementation of personal data sovereignty and dynamic consent (de Andrade Cardieri & Zaina, 2018; ISO/IEC, 2018).

## 7.15 Results and Implementation Summary

Section 7 demonstrates how the governance directives articulated in Section 6 are operationalized within Consentio. Policies are decomposed into concrete, testable requirements in a traceability matrix and expressed through both static design artifacts, such as use-case diagrams and a domain model (including **Study, DynamicConsentForm, ConsentPrivacyQuantificationScore, ConsentTransaction,**

**DataPrivacy, StudyVersion, StudySuspension, StudyOutcome, Notification, ContactList, and ProfileImage**), and through dynamic lifecycle behaviours, encoded as finite-state diagrams that distinguish preparatory states (e.g., *Stopped*), runtime suspensions (*Paused*), and terminal conditions (*Ended*). Ambiguity is reduced via formal rules written in propositional logic with selective first-order quantification; core predicates (e.g., $S_o \rightarrow (I_a \wedge P_a)$ for dual approval before starting a study, $S_d \rightarrow (\neg R_o \wedge \neg D_o)$ to block recruitment during drafting, and $D_share \rightarrow (P_g \wedge \neg P_r \wedge D_a)$ to constrain data sharing by purpose and revocation status) define admissible transitions and safety invariants. These rules are enforced in the user-interface and service layers via Angular route guards, validators and workflow constraints, so that only lawful paths, publication, start, pause, stop, end, consent, revocation, re-consent and anonymized sharing, are reachable. Auditability is achieved through append-only records for approvals, consent events and data-sharing actions, complemented by tamper-evident receipts in the ledger-backed deployment. In this way, Section 7 delivers an executable governance pipeline that connects high-level policy to verifiable platform behaviour.

## 7.16 Limitations

While the implementation demonstrates the feasibility of governance-to-platform translation, several limitations warrant attention. The formal layer uses propositional logic with limited first-order quantification; temporal constraints are represented through event histories rather than full temporal or deontic logic, which restricts expressiveness for complex proofs or normative conflicts. Metadata leakage remains a concern: even when rich artifacts are stored off-chain, audit logs can reveal timing or usage patterns. The prototype prioritizes correctness and auditability over throughput; systematic performance and scalability evaluations, especially in multi-institutional contexts, are deferred to future work. Domain scope is currently tuned to public-health research; other sectors may require new roles, policies or interoperability standards. Finally, the platform assumes partial reliability from external components (identity providers, off-chain storage, institutional review processes) that remain outside its direct control.

To address these limitations, future work will extend the interface to deepen governance support for principal investigators, institutional review boards and auditors by providing compliance dashboards, structured review workflows and traceable decision dossiers. Third-party custodians will gain consent-status verification APIs and clearer accountability dashboards, while audit integration will be automated for processor events. Field evaluation, via clinical and public-health pilots, will test usability, governance efficacy and compliance under real conditions, including longitudinal analyses of revocation and re-consent dynamics and cross-jurisdictional policy packs (EU, Canada, United States). Technical enhancements will include lightweight temporal modelling for critical flows, policy-lifecycle tooling with semantic versioning and rollback, standards-based interoperability via FHIR/HL7 connectors, stronger privacy safeguards (e.g., differential privacy and consent-aware minimization), performance benchmarking, and hardening against metadata leakage or key-management failures.

## 7.17 Discussion

Future interface work will deepen governance support for oversight roles, including PI dashboards for compliance posture, consent dynamics, and audit alerts, and structured, traceable review workflows for IRBs and auditors that produce decision trails and audit dossiers with embedded proofs, hashes, and receipts. Third-party custodians will be supported through consent-status verification APIs and dashboards that clarify processing scope, retention limits, and accountability obligations, alongside programmatic audit integration for processor events. Deployment will shift from demonstrator to field evaluation through partnered clinical and public-health pilots that test usability, governance efficacy, and compliance under real conditions, including longitudinal analysis of revocation and re-consent dynamics and cross-jurisdictional policy packs for the European Union, Canada, and the United States, complemented by external audits and red-team exercises. Technically, planned work includes lightweight temporal modelling for critical flows, policy lifecycle tooling with semantic versioning and rollback, stronger interoperability via FHIR/HL7 connectors, expanded privacy safeguards such as differential privacy and consent-aware

minimization, performance benchmarking and scaling of event processing, and hardening against metadata leakage and key-management failures (Health Level Seven International, 2020).

### 7.17.1 Contributions

This section contributes an executable governance pipeline that connects policy to formal rules, system design, code-level enforcement, and verifiable evidence. It operationalizes dynamic consent as enforceable predicates with audit-ready proofs, aligning participant-centric consent management with privacy engineering expectations and verifiable oversight(Sheehan et al., 2019; Zhang et al., 2004). Methodologically, it provides a repeatable translation sequence from traceability to diagrams to logic to runtime guards, consistent with "privacy by design and by default" obligations (European Parliament and of the Council of 27 April 2016, 2016; Rossi & Palmirani, 2017). It also adopts compensating transactions for multi-step operations to preserve consistency under failure in distributed services (Microsoft Learn, 2026). Conceptually, CPIQ is introduced as a first-class, versioned artifact that makes privacy risk legible and actionable for participants and oversight roles, and supports re-consent and DPIA-like triggers when risk changes (European Parliament and Council of the European Union, 2016e; European Parliament and Council of the European UnionEuropean Parliament and Council of the European Union, 2016; Williams et al., 2015). Technologically, the platform combines tamper-evident auditability with minimization by keeping rich artifacts off-chain while committing cryptographic digests and minimal facts to the audit layer, supported by endorsement and private-scope mechanisms (Androulaki et al., 2018a; Six et al., 2022; Teare et al., 2020). Practically and regulatorily, it enforces least-privilege, minimum-necessary constraints, auditable breach workflows, and explicit mappings from regulatory duties to predicates and events (Calder, 2019; European Parliament and Council of the European Union, 2016g; European Parliament and of the Council of 27 April 2016, 2016; Office of Privacy Commissioner of Canada, 2018; Technical Committee ISO/IEC JTC 1, 2022; Technical Committee ISO/TC 215, 2021; Tovino, 2017; U.S. Food and Drug Administration, 2026d).

### 7.17.2 Answer to RQ2: Governance-to-Platform Transcription with a Tamper-Evident Audit Layer

This work proposes a substrate-agnostic method that converts formal governance duties into a single library of executable predicates that gate the UI and APIs, and that is mirrored by an audit substrate that refuses non-conformant transactions and emits signed, time-stamped evidence for conformant ones. Duties are factored in the traceability matrix and transcribed into guards such as So → (Ia ∧ Pa) for dual approval before start, Sd → (¬Ro ∧ ¬Do) to block recruitment and data operations in draft, and Dshare → (Pg ∧ ¬Pr ∧ Da) to constrain sharing by purpose, revocation status, and anonymization, with lineage expressed through constraints such as ∀p (Pe(p) → Pi(p)). Multi-party approval is enforced via endorsement checks, identity and roles are bound to least-privilege permissions, sensitive artifacts are stored off-chain while hashes and minimal facts anchor verifiability, and resilience is provided through idempotent operations and compensating transactions; verification combines property-based transition testing, scenario tests for end-to-end governance flows, and audit reconstruction that answers who did what, when, and under which policy.

## 7.18 Conclusion

By integrating policy decomposition, formal specification, code-level enforcement and tamper-evident auditing, Section 7 bridges the gap between abstract governance frameworks and operational systems. The proposed pipeline demonstrates that dynamic consent can be made auditable, revocable and compliant when backed by formal predicates and ledger technology. Although the implementation is formative and tailored to public health research, its principles are broadly applicable: other domains can adopt the same recipe, policy tracing, logic translation, guard implementation, and ledger anchoring, to build trustworthy data governance platforms. Together with the methodological extensions outlined above, this work lays a foundation for future research and development in participant-centred data sharing and regulatory compliance.

# 8 Quantitative Assessment of Consentio Dynamic Informed Consent Platform Based on Participants' Surveys

## 8.1 Introduction

The growth of dynamic consent systems has transformed the management of research studies and clinical trials. Such systems enable participants to provide fine-grained consent for various data uses and to modify their choices over time. Consentio is a web-based platform designed to facilitate dynamic consent for biomedical research. To determine whether the platform meets the expectations of prospective users, a series of surveys was conducted. These instruments measured usability, digital skills, computer self-efficacy, customer satisfaction and overall sentiment. This section presents the results of the surveys, interprets their implications for the Consentio platform, and situates the findings within the existing literature.

Usability was assessed with the Post-Study System Usability Questionnaire (PSSUQ) (Lewis, 2011; T, 2026), a 16-item instrument developed by IBM researcher Jim Lewis in the late 1980s and published in 1995. The PSSUQ uses a seven-point response scale (1 = strongly agree, 7 = strongly disagree) and yields three subscales: system usefulness (items 1–6), information quality (items 7–12), and interface quality (items 13–15). Normative data suggest that PSSUQ scores below 3 are desirable.

Digital skills were measured using the Internet Skills Scale (ISS). Developed in 2014 by Van Deursen, Helsper and Eynon, the ISS aims to capture a wide spectrum of digital abilities, from basic operational tasks to advanced content creation, and has been applied internationally (Digital Inclusion Index, 2021; van Deursen et al., 2015). The authors note that earlier measures of digital skills were overly simplistic; therefore, the ISS distinguishes five domains: operational, information navigation, social, creative and mobile skills (Digital Inclusion Index, 2021). Later adaptations introduced an "automation" domain to cover the Internet of Things (Digital Inclusion Index, 2021). Each item is rated on a scale from 0 ("not at all") to 5 ("very much"), allowing for the calculation of domain-specific and overall scores.

Self-efficacy with computing was assessed using the Computer User Self-Efficacy (CUSE) scale. This 30-item instrument quantifies users' confidence in their ability to perform computer-related tasks. Cassidy and Eachus (2002) developed the CUSE and reported excellent psychometric properties. Respondents rate each item on a six-point Likert scale.

Customer satisfaction was measured using a short questionnaire that asked participants to rate their satisfaction with the system's usability, ease of use, the extent to which it met their needs and their likelihood of continued use. Qualitative questions captured the features participants used, suggestions for improvement and open-ended comments.

To gauge overall loyalty, a Net Promoter Score (NPS) survey was administered. The NPS is an index ranging from –100 to +100 that measures respondents' willingness to recommend a product or service (Fisher & Kordupleski, 2019; Nadanyiova et al., 2022). It classifies respondents into Promoters (scores 9–10), Passives (scores 7–8) and Detractors (scores 0–6). The score is computed by subtracting the percentage of detractors from the percentage of promoters. Scores above 20 are considered favourable and scores above 50 are regarded as excellent (Reichheld, 2006).

Finally, a demographic survey collected information on age, gender, employment status, education, research experience, and self-rated computer proficiency. The following sections describe the methodology used to collect and analyse the data, present the results for each survey, and discuss the implications for the Consentio platform.

## 8.2 Research Questions

This section examines how dynamic informed-consent features and a ledger-backed audit layer in Consentio shape users' trust, perceived usability, and motivation to participate in public-health research. We adopt a critical-realist stance and triangulate three lenses: (i) quantitative surveys (PSSUQ, ISS, CUSE, satisfaction items, NPS), (ii) qualitative interviews/open-ended feedback from researchers and participants, and (iii) a close reading of platform workflows across the consent lifecycle and audit trail.

### 8.2.1 RQ1 — Research Operations and Ease of Use (Researcher View). How Can Platforms Like Consentio Enhance the Ease of Publishing and Managing Public Health Studies?

Scope: Researcher-facing workflows (study creation, consent configuration, recruitment/participant tracking, researcher–participant communications).

Measures & sources: PSSUQ subscales; researcher-oriented themes (centralized study management, customization/personalization, notification & data-presentation preferences); workflow analysis (permission states, lifecycle guards).

Interpretation criteria: Evidence of reduced coordination overhead, clearer permission states, and faster iteration on study artifacts; localization of residual friction via open-ended feedback (e.g., filtering, dashboards, timelines).

### 8.2.2 RQ2 — Dynamic Consent, UX, And Willingness to Participate (Participant View). How Do Dynamic-Consent Features and User Experience Affect Willingness to Enroll (And Remain) In Studies?

Scope: Enrollment intent and sustained participation as shaped by usability and digital ability.

Measures & sources: Satisfaction and NPS signals conditioned by usability (PSSUQ) and digital ability (ISS/CUSE); participant-oriented themes (data control—with caveats; transparency that is explained, not assumed; usability that protects informedness).

Interpretation criteria: Whether perceived usability and explainability translate into higher willingness to enroll/continue; identification of interface or comprehension gaps that suppress motivation.

### 8.2.3 RQ3 — Ledger-Backed Audit and Perceived Empowerment. How Does the Use of Blockchain (Tamper-Evident Audit) Empower Consent Processes and Give Users Control Over Their Data?

Scope: Platform affordances: granular/revocable permissions; immutable, participant-verifiable audit trails; provenance supporting re-contact and governed secondary use.

Measures & sources: Participant and researcher reflections on trust and control; inspection of audit-trail visibility within consent workflows.

Interpretation criteria: Whether these affordances produce *felt* trust and perceived control, where additional explanation, interface design, or policy scaffolding is required to make ledger guarantees legible and meaningful in practice.

## 8.3 Methods

This section details the study design and analytic approach used to evaluate the Consentio platform. It first describes the participant sample and recruitment context, then documents the measurement instruments, PSSUQ for perceived usability, the Internet Skills Scale (ISS) for digital ability, the Computer User Self-Efficacy (CUSE) scale for confidence with computing tasks, a brief customer-satisfaction questionnaire, and a Net Promoter Score (NPS) item. Data handling procedures are then outlined, including export from Qualtrics, cleaning, scoring, and transformations (notably, PSSUQ items were oriented so that higher values reflect better usability). The section concludes with a discussion of the statistical methods employed for descriptive estimates and internal consistency reliability, as well as the qualitative treatment of open-ended responses. All procedures were conducted in accordance with the institutional research ethics and data governance principles articulated earlier in the thesis.

### 8.3.1 Participants

Participants were recruited from the intended user base for Consentio. The demographic survey yielded five valid responses. Respondents ranged in age from 18-24 years to 25-34 years, with the majority (80 %)

in the 25-34 age group. Four respondents identified as women and one as a man. Four were full-time students, and one was employed full-time. Educational attainment was high: three held postgraduate degrees, one had some college education and one selected "other" for education. Three respondents self-rated their computer proficiency as advanced, one as intermediate and one as expert. All participants resided in Canada and reported prior experience with electronic health records or data management. Recruitment through word of mouth accounted for the majority of participation (four respondents), with social media contributing one respondent.

### 8.3.2 Study Procedure and Participant Experience

This user-study was designed to evaluate the Consentio platform in a way that approximated real-world consent management. After obtaining institutional approval, we recruited a convenience sample of public-health researchers and lay participants who were prospective data subjects. Individuals met either in person in a controlled laboratory environment or remotely via Zoom/MS Teams, reflecting the hybrid nature of modern research engagements. Each session lasted approximately 60–90 minutes and was supervised by a researcher who provided technical support and observed task completion without intervening in decision-making.

### 8.3.3 Orientation And Pre-Test Survey

Upon arrival, participants received a brief overview of the study's purpose and the core features of dynamic consent. They were then asked to complete an online pre-test survey hosted in Qualtrics. This instrument collected demographic information (e.g., age, gender, education, employment status) and baseline measures of digital competency and self-efficacy. In particular, the Internet Skills Scale (ISS) and Computer User Self-Efficacy (CUSE) instruments were used to establish participants' existing ability to navigate online tools. This pre-session questionnaire ensured that differences in later evaluations could be interpreted in light of participants' prior experience with technology.

### 8.3.4 Hands-On Tasks in The Consentio Platform

After the pretest, participants logged in to the Consentio platform under the researcher's guidance. They were instructed to complete a series of structured tasks that mirrored both the participant's (data subject) and the researcher's perspectives. The task list was based on the original project proposal and was designed to exercise the end-to-end consent lifecycle. Typical tasks for data-subjects included:

- Account Creation and Onboarding: Sign up for Consentio using a pseudonym, and complete the onboarding tutorial.
- Study Enrolment: Browse a public-health study description, review the purpose, data-collection methods and potential risks, and decide whether to grant consent for specific data categories. Participants could experiment with fine-grained consent options (e.g., share only de-identified data or allow re-contact for ancillary studies).
- Consent Review and Modification: Return to the study dashboard to view the audit trail of past consent decisions and exercise the right to withdraw or amend consent. Participants were asked to change one or more permissions and confirm that the updated settings were correctly recorded on the blockchain ledger.
- Data-subject Requests: Submit a request to access personal data held by the study team or to see how their contributions had been used, illustrating the platform’s support for data-subject rights under regulations such as the GDPR.

From the researcher's perspective, participants with a public-health background were given a second set of tasks to complete after logging in with a researcher role. These tasks included:

- Study Creation: Create a new study template, define data-collection instruments and specify consent options using the platform’s wizard.
- Participant Management: Review incoming consent records from mock participants, reply to participants, request re-consent, and respond to withdrawal requests.

- Audit and reporting: access the ledger-backed audit trail to verify that consent transactions were immutable and generate a summary report of consents received.

Throughout the hands-on session, participants were encouraged to think aloud so that researchers could capture usability issues and gauge the clarity of the interface. The tasks were designed to be completed sequentially, but participants were free to explore other features if they wished. The researcher noted any errors or points of confusion but did not provide direct assistance unless technical problems occurred.

### 8.3.5 Post-Session Surveys and Debriefing

Immediately after completing the tasks, participants were directed back to Qualtrics to complete a post-session questionnaire. This instrument comprised several standardized scales: the Post-Study System Usability Questionnaire (PSSUQ) to assess perceived usability at both the task and interface levels, and a brief customer-satisfaction module evaluating how well the platform met their needs. An NPS (Net Promoter Score) item captured participants' willingness to recommend Consentio to peers, and open-ended questions solicited qualitative feedback. Administering these instruments immediately after the core workflows minimized recall errors and allowed participants to reflect on their interaction while it was still fresh. Response scales were harmonized so that higher values represented more positive evaluations, and internal-consistency reliability was assessed during analysis.

After completing the surveys, participants were debriefed about the study's aims and the hypothetical nature of the data they interacted with. In the case of remote sessions, a secure screen-sharing protocol ensured that researchers could observe task completion without capturing any personal identifiers. Participants were thanked for their time and received compensation as specified in the ethics protocol. The resulting dataset contained pre- and post-test measures, task observations and open-ended comments that together provided a rich picture of the Consentio user experience.

Finally, immediately after completing the task sequence, participants took part in a brief, semi-structured interview (10–15 minutes) conducted in person or via Zoom, depending on their session

modality. With prior consent, interviews were audio-recorded and later transcribed verbatim. The guide probed perceptions of autonomy and control (e.g., clarity of revocation, visibility of consent state and history), trust and accountability (e.g., auditability and role of the ledger), usability and cognitive load (e.g., comprehension of study information and consent options), and anticipated adoption (e.g., fit with everyday practices, perceived barriers and enablers). Interviews served to contextualize survey responses and interaction traces, allowing us to examine how participants interpreted specific interface affordances and governance cues encountered during the tasks. Transcripts were analysed using reflexive thematic analysis, with codes developed iteratively from both the interview guide and emergent concepts in the data; summaries were then triangulated with pre/post survey measures and observed task outcomes to generate a consolidated account of user experience, perceived risks and benefits, and the perceived legitimacy of dynamic consent in public health research settings.

## 8.4 Survey Instruments

This subsection outlines the standardized questionnaires used to capture complementary facets of users' interaction with Consentio. We combined the Post-Study System Usability Questionnaire (PSSUQ) to assess perceived usability at the task and interface levels, the Internet Skills Scale (ISS) to profile baseline digital ability that may condition usability judgments, the Computer User Self-Efficacy (CUSE) scale to measure confidence with common computing tasks, a brief customer-satisfaction module to gauge attitudinal outcomes, and a single-item Net Promoter Score (NPS) to index advocacy and loyalty intention. Instruments were administered in Qualtrics immediately after core workflows to minimize recall bias; wording was retained, with minor adjustments to accommodate platform terminology. Response scales were retained, with item polarity harmonized so that higher values consistently indicate more positive evaluations. Open-ended prompts accompanied the structured items to contextualize quantitative results with brief qualitative feedback.

### 8.4.1 Post-Study System Usability Questionnaire (PSSUQ)

The PSSUQ consists of 16 positively worded items, each rated on a seven-point scale where 1 indicates strong agreement and 7 indicates strong disagreement. The instrument yields a global usability score and three subscales: system usefulness, information quality and interface quality. Lower scores indicate better perceived usability; benchmark data suggest that scores around 2.8 represent average usability. In this study, the PSSUQ was adapted for use within the Consentio post-task survey; some items may appear under different question identifiers in the dataset.

### 8.4.2 Internet Skills Scale (ISS)

The ISS measures digital ability across five domains: operational skills (e.g., connecting to the internet, managing files), information navigation (e.g., searching and verifying sources), social skills (e.g., managing contacts and sharing content), creative skills (e.g., producing and editing content) and mobile skills (e.g., using mobile devices and apps). The instrument's development emphasized a comprehensive yet nuanced approach to digital ability[1]. Respondents rate items on a six-point scale from 0 (no proficiency) to 5 (high proficiency).

### 8.4.3 Computer User Self-Efficacy (CUSE) Scale

The CUSE is a 30-item scale designed to quantify confidence in using computers. Each item is rated on a six-point Likert scale ranging from "strongly disagree" to "strongly agree". (Cassidy & Eachus), In our implementation, an introductory question identified the device used (e.g., code names "0004", "0005", "R001"), and the subsequent questions corresponded to CUSE items. Items were recorded with numerical values (0-6) for analysis.

### 8.4.4 Customer Satisfaction Questionnaire

This brief questionnaire contained single-choice questions assessing satisfaction with the system's usability and ease of use, how well the system met participants' needs and the likelihood that they would continue using the platform. Response options ranged from "*very satisfied*" to "*very dissatisfied*", "*very easy*" to

"*very difficult*", "*exceptionally well*" to "*not at all*", and "*very likely*" to "*very unlikely*". Additional questions captured the features participants used, improvement suggestions and open-ended comments.

### 8.4.5 Net Promoter Score Survey

The NPS survey asked: "How likely is it that you would recommend Consentio to a friend or colleague?" Respondents selected a score from 0 to 10. According to Qualtrics' NPS guide, scores of 9–10 indicate promoters, scores of 7–8 indicate passives, and scores of 0–6 indicate detractors. The Net Promoter Score is computed by subtracting the percentage of detractors from the percentage of promoters. A score above 20 is considered favorable and a score above 50 is rated excellent. Table 13 below presents more detailed information and general details about each survey.

*Table 12 - Survey instrument details.*

| Survey Instrument | Items & Structure | Scale Used | Example Content & Response Categories |
|---|---|---|---|
| Post-Study System Usability Questionnaire (PSSUQ) | 16 items grouped into three usability dimensions – *System Usefulness* (items 1-6), *Information Quality* (items 7-12) and *Interface Quality* (items 13-15), plus a global satisfaction item | 7-point Likert scale; range 1–7, where lower scores indicate stronger agreement (1 = most positive/strongly agree, 7 = most negative/strongly disagree). Score 4 is neutral | Statements ask about satisfaction with ease of use, ability to complete tasks quickly, clarity of error messages and help information, pleasantness of the interface, and whether the system has all necessary functions; includes an optional comments field |
| Internet Skills Scale (ISS) | 34 items across five skill domains: *Operational* (e.g., downloading files, using browser tabs), *Information navigation* (e.g., selecting keywords, verifying sources), *Social* (e.g., knowing what information to share online), *Creative* (e.g., combining or editing online content, understanding licenses) and *Mobile* (e.g., installing apps, managing costs) | 5-point Likert scale; responses range from "not at all true for me" to "very true for me" with a neutral "neither true nor untrue" option | Items assess confidence with basic internet operations, difficulties finding or verifying information, ability to manage privacy and social interactions, capacity to create and edit digital content, and mobile app skills |
| Computer User Self-Efficacy (CUSE) Questionnaire | 30 self-efficacy items (plus background questions) measuring attitudes toward computer use (confidence, comfort, anxiety, productivity); some negatively worded items require reverse scoring | 6-point Likert scale ranging from 1 = strongly disagree to 6 = strongly agree | Items include "Most difficulties I encounter when using computers I can usually deal with," "I am very unsure of my abilities to use computers," "Computers frighten me," and "Computers make me much more productive." Responses capture degrees of confidence, fear, frustration and enjoyment |
| Customer Satisfaction Questionnaire | 9 items evaluating satisfaction with the Consentio platform; includes closed-ended and open-ended questions | Categorical scales rather than numeric Likert: satisfaction (Very Satisfied → Very Dissatisfied), ease of navigation (Very Easy → Difficult), how well the platform meets needs (Exceptionally Well → Poorly), likelihood to recommend (Very Likely → Very Unlikely); multi-select questions on useful features and suggested improvements; free-text comment field | Asks "Overall, how satisfied are you with Consentio?", "How easy was it to navigate our platform?", "How well does our platform meet your needs?", "What features do you find most useful?", (e.g., Study Management, Dynamic Consent Management, Chat), "What improvements would you suggest?", (options include feature enhancement, user interface improvement, customer support), and a prompt for additional comments |
| Net Promoter Score (NPS) Survey | 3 items: (1) NPS rating; (2) primary reason for the rating; (3) suggestion to improve experience | NPS rating uses an 11-point scale (0–10); respondents scoring 9–10 are classified as promoters, 7–8 as passives, and 0–6 as detractors; the NPS score is the percentage of promoters minus the percentage of detractors | The main question asks: "*On a scale from 0 to 10, how likely are you to recommend Consentio to a friend or colleague*?" accompanied by open-ended questions for reasons and suggestions |
| Demographic Survey | 13 questions capturing participant characteristics and prior experiences | Categorical responses rather than rating scales; options include age, gender, occupation, education level, technology proficiency, residency, and experience with health data management platforms. | Respondents select the category that best describes them and can optionally describe their experience with health data platforms |

## 8.5 Data Processing and Analysis

The raw survey data were stored in comma-separated value (CSV) files exported from Qualtrics. Each file contained two metadata rows: an initial row of human-readable column headings and a second row describing Qualtrics import identifiers. For analysis, the first two rows were removed so that data frames contained only participant responses. Analyses were performed using Python (pandas and NumPy). The following procedures were applied:

- Identification of Numeric Items – For the PSSUQ, ISS and CUSE datasets, columns with question identifiers (e.g., Q1_1, Q9_1) were extracted. Response strings were converted to numeric values, with non-numeric responses coded as missing values. For the CUSE scale, only items that clearly followed the Likert-type numbering were included.
- Descriptive Statistics – for each item, the mean and standard deviation were computed across all valid responses. Overall scores for each participant were calculated by taking the mean of the available numeric items, and the mean and standard deviation of these overall scores were then computed.
- Customer Satisfaction Counts – for each of the satisfaction items (Q1, Q2, Q4 and Q5), categorical responses were tallied.
- Net Promoter Score – responses to the NPS rating were classified as promoters (9–10), passives (7–8) or detractors (0-6) based on Qualtrics' definitions. The Net Promoter Score was then calculated.
- Demographics – for each demographic question, the frequency of each response option was tabulated. Free-text answers to open-ended questions were summarized qualitatively.

The following section presents the results of these analyses in tabular form. Tables use concise phrases and numbers, while the narrative highlights key findings.

### 8.5.1 Reliability and Confidence Intervals

To understand how the sample means might generalize to a larger population, we instead compute 95 % confidence intervals (CIs)(Kelley & Pornprasertmanit, 2016) for the composite scores. For each instrument,

the per-participant mean is calculated across items; the sample mean ($\bar{x}$), standard deviation $s$and sample size $n$are then used to derive the CI as $\bar{x} \pm t_{n-1,0.975} \times s/\sqrt{n}$. CIs provide a range within which the population mean is likely to fall, given the observed data and the t-distribution. This method is appropriate for extrapolating descriptive statistics from small samples.

## 8.6 Results

Results are reported in the order of the study workflow. The descriptive characteristics of the sample are presented first to provide context for the interpretation. Scale-specific findings then follow for the PSSUQ (with directionally transformed scores where higher indicates better usability), ISS, and CUSE, including item-level means, standard deviations, and reliability coefficients where estimable. Summary outcomes for customer satisfaction and the Net Promoter Score are subsequently provided, complemented by a brief synthesis of open-ended feedback. Given the small amount of missingness in responses, the emphasis is on transparent descriptive and inferential clarity, as well as the reproducibility of calculations.

### 8.6.1 Demographic Characteristics

Ten respondents completed the demographic questionnaire: five data subjects and five researchers. The sample remains relatively homogeneous, skewing young and highly educated. Age clustered in the 25–34 range (18–24: 3; 25–34: 7). gender was predominantly women (8) with two men. Employment status was chiefly student (9) with one full-time employee; note that several researchers were graduate-student researchers, which explains the student majority. Education was high overall (Postgraduate degree: 6; Some college: 2; Undergraduate degree: 1; Other: 1). Computer proficiency was self-rated as Advanced (7), Expert (2), and Intermediate (1). All respondents reported residence in Canada, and all reported prior research experience. Recruitment was informal: Word of mouth (8), social media (1), Email (1). This profile, young, female-leaning, student-heavy, high digital ability, and research-experienced, supports the strong usability scores observed later but also limits generalizability to populations with lower digital literacy or different roles.

*Table 13 - Demographics survey results.*

| Demographic Variable | Distribution |
|---|---|
| Age Group (Q1) | 18–24 (3), 25–34 (7) |
| Gender (Q2) | Women (8), Men (2) |
| Employment Status (Q4) | Student (9), Employed (full-time) (1) |
| Education (Q6) | Postgraduate degree (6), Some college (2), Undergraduate degree (1), Other (1) |
| Computer Proficiency (Q8) | Advanced (7), Expert (2), Intermediate (1) |
| Residence (Q9) | Canada (10) |
| Prior Research Experience (Q10) | Yes (10) |
| Recruitment Source (Q12) | Word of mouth (8), social media (1), Email (1) |

### 8.6.2 Post-Study System Usability Questionnaire

Ten respondents (five data subjects and five researchers) completed the PSSUQ. Scores use a 1–7 scale, with higher values indicating better usability. Item-level means and standard deviations are shown below using Q1–Q19 labels for clarity.

*Table 14 - PSSUQ Results.*

| PSSUQ Item | Item | Mean | SD |
|---|---|---|---|
| 1 | Overall satisfaction | 1.60 | 0.70 |
| 2 | Interface reflects real-world needs | 1.80 | 0.92 |
| 3 | Navigation is consistent | 1.40 | 0.84 |
| 4 | System characteristics meet needs | 1.60 | 0.52 |
| 5 | Errors are handled properly | 1.70 | 0.82 |
| 6 | Learning to operate the system | 1.70 | 0.48 |
| 7 | Efficiency of use | 1.30 | 0.48 |
| 8 | Tasks are easy to accomplish | 1.40 | 0.52 |
| 9 | Recovery from errors | 3.20 | 2.30 |
| 10 | System helps recover from mistakes | 1.90 | 0.99 |
| 11 | System is easy to use | 2.00 | 0.94 |
| 12 | Access to support information | 2.00 | 0.47 |
| 13 | Information helps recover from errors | 1.50 | 0.53 |
| 14 | System is pleasant to use | 1.60 | 0.52 |
| 15 | Completeness of information provided | 2.20 | 0.79 |
| 16 | System meets all requirements | 1.90 | 0.57 |
| 17 | Overall, system meets needs | 1.90 | 0.99 |
| 18 | System has all necessary functions | 1.90 | 0.74 |
| 19 | System handles information securely | 1.90 | 0.57 |

Means are computed on the reversed 1–7 scale (8 – rating). Lower values indicate more positive perceptions (1 = strongly agree). The composite global score across all items and respondents was M = 1.82, SD = 0.45, with a 95 % CI of 1.50–2.14.

#### 8.6.2.1 Overall Statistics

Across all 10 respondents, the PSSUQ items were reverse-scored so that higher values indicate better usability (rating_reversed = 8 – raw rating). On this reversed scale the per-person global mean was 1.82 (SD = 0.45), and the 95 % confidence interval was 1.50–2.14. Lower values correspond to stronger agreement with positive statements, so this means reflects a high level of perceived usability. The item-level pattern shows most means between 1.3 and 2.7; the only clear outlier was Q9 (recovery from errors, M = 3.20), suggesting that error handling and recovery cues warrant improvement.

### 8.6.3 Internet Skills Scale

Ten respondents completed the ISS. On the 0–5 scale, the overall mean across all items (per-person average) was 3.75 ± 0.30, indicating moderate to high digital skills in this sample.

#### 8.6.3.1 Domain pattern (Q1–Q34)

ISS domains showed the expected stratification, characterized by very high operational and mobile skills, strong but more variable information navigation, and lower creative/social skills. Research matches showed that operational skills tend to be more developed than creative or evaluative skills(Hargittai et al., 2019; Neves et al., 2013).

*Table 15 - ISS results.*

| Domain (Items) | K | Mean | Sd (Per-Person Means) |
|---|---|---|---|
| Operational (Q1–Q8) | 8 | 4.97 | 0.05 |
| Info Navigation (Q9–Q10) | 2 | 4.25 | 0.98 |
| Creative/Social (Q11–Q18) | 8 | 1.54 | 0.89 |
| Mobile (Q19–Q23) | 5 | 4.70 | 0.32 |
| Advanced Creative (Q24–Q34) | 11 | 3.95 | 0.46 |

Respondents are at (or near) ceiling for routine operations (Q1–Q8) and are highly comfortable with mobile tasks (Q19–Q23). Information search/evaluation (Q9–Q10) is strong on average but shows wide individual variation. In contrast, creative/social skills (Q11–Q18) are notably weaker, with substantial dispersion, consistent with prior findings that content production and socially mediated tasks often lag behind basic proficiency. Advanced creative tasks (Q24–Q34), such as editing, formatting, or more complex content handling, sit in the mid-high range but below operational/mobile skills.

These results suggest targeted support would be most impactful in content creation, sharing, and socially mediated workflows (e.g., lightweight tutorials, templates, and step-by-step guides for producing and assessing research-related materials), while maintaining current strengths in operational/mobile use.

### 8.6.4 Computer User Self-Efficacy (CUSE)

Ten respondents completed the CUSE scale. On the 0–6 metric, the overall mean (per-person average) was 2.96 ± 0.29, indicating moderate confidence with everyday computing tasks in this sample.

#### 8.6.4.1 Item Pattern (highs vs. lows)

The highest means concentrate in routine productivity and web use: Q14 (using internet browsers) 5.2, Q35 (using graphical interfaces) 5.0, Q20 (navigating menus) 4.6, Q26 (using web search engines) 4.3, Q10 (word-processing) 4.2.

The lowest means cluster in programming, troubleshooting, and specialized tooling: Q30 (debugging) 1.1, Q21 (writing simple programs) 1.1, Q27 (programming macros) 1.5, Q12 (spreadsheet operations) 1.6, Q23 (graphic design tools) 1.7.

*Table 16 - CUSE survey results.*

| Item | Brief label (CUSE item meaning) | Mean | SD |
|---|---|---|---|
| Q9 | Can resolve most computer difficulties | 3.20 | 1.81 |
| Q10 | Computers are easy to use | 4.20 | 1.40 |
| Q11 | Unsure about computer ability | 4.20 | 2.10 |
| Q12 | Struggle with most software | 1.60 | 0.97 |
| Q13 | Computers feel intimidating | 3.20 | 2.25 |
| Q14 | Enjoy using computers | 5.20 | 1.32 |
| Q15 | Computers hinder learning | 2.70 | 1.83 |
| Q16 | Few issues with legacy/command-style software | 2.30 | 1.34 |
| Q17 | Computers increase productivity | 3.50 | 2.12 |
| Q18 | Difficulty learning new software | 3.60 | 1.51 |
| Q19 | Most software is easy | 2.10 | 1.60 |
| Q20 | Confident using computers | 4.60 | 0.70 |
| Q21 | Hard to make the computer do what I want | 1.10 | 0.32 |
| Q22 | Computers can be confusing | 3.60 | 1.71 |
| Q23 | Prefer not to learn computers | 1.70 | 1.16 |
| Q24 | Easy to learn new software | 2.90 | 1.91 |
| Q25 | Waste time struggling | 2.40 | 1.26 |
| Q26 | Computers make learning interesting | 4.30 | 1.25 |
| Q27 | Frequent problems using computers | 1.50 | 1.43 |
| Q28 | Some software makes learning easier | 4.00 | 2.16 |
| Q29 | Computer jargon is confusing | 3.90 | 2.23 |
| Q30 | Computers are too complicated | 1.10 | 1.37 |
| Q31 | Rarely enjoy using computers | 3.60 | 1.96 |
| Q32 | Computers aid learning | 3.50 | 2.22 |
| Q33 | Unexpected behaviour I can’t explain | 2.00 | 1.63 |
| Q34 | Low perceived computer competence | 1.90 | 1.29 |
| Q35 | Computers save time | 5.00 | 1.49 |
| Q36 | Computers are frustrating | 1.90 | 1.29 |
| Q37 | Consider self a skilled user | 2.30 | 2.41 |
| Q38 | Fear pressing wrong button / damaging system | 1.70 | 1.83 |

Participants feel competent with everyday GUI and web tasks (browsers, menus, search, word-processing), while confidence drops sharply for programming/scripting, debugging, some spreadsheet operations, and graphic-design tools. Given the very low internal consistency across all items, aggregated CUSE scores should be treated cautiously. A clustered reading (e.g., "*everyday productivity*" vs. "*programming/scripting*" vs. "*specialized tools*") is more informative for identifying targeted training, for example, lightweight tutorials or just-in-time help for spreadsheets, data analysis, and basic scripting, while maintaining current strengths in routine tasks.

### 8.6.5 Customer Satisfaction

Ten respondents completed the customer satisfaction questionnaire. Satisfaction was uniformly positive: all respondents reported being "*Satisfied"* or "*Very Satisfied*", rated the platform "*Easy"* or "*Very Easy*" to use, indicated it met their needs "*Very Well*" or "*Exceptionally Well*", and were "*Likely*" or "*Very Likely*" to continue using it. Open-ended remarks again highlighted the value of centralized study/consent management and intuitive workflows, while suggesting refinements (e.g., clearer help/error messaging, filtering, dashboard customization, dark mode).

*Table 17 - CSAT survey results.*

| CSAT item | Correct source column(s) in your exports | Observed distribution | Why does it look "unanimously positive" |
|---|---|---|---|
| Q1 Overall satisfaction | Q1 (all respondents) | Very Satisfied = 5; Satisfied = 5 | Everyone selected one of the two top categories; no Neutral/negative responses were recorded. |
| Q2 Ease of navigation | Q2 (all respondents) | Very Easy = 6; Easy = 4 | Again, everyone selected a positive category. |
| Q3 Meets needs | DataSubjects: Q3; Researchers: Q5 | Very Well = 7; Exceptionally Well = 3 | This item is split across two columns because the researcher survey version placed it in Q5, while the participant/data-subject version placed it in Q3. When harmonized, your counts match. |
| Q4 Recommend to others | Q4 (all respondents) | Very Likely = 6; Likely = 4 | Everyone selected a positive category. |

Open-ended feedback shows respondents most often used study management, dynamic consent management, and the chat module. Requested improvements clustered around UI polish and guidance,

richer in-app help and clearer error/recovery cues, alongside more powerful filtering and study organization, a dark mode, and greater dashboard customization. Together, these suggestions are concrete and readily actionable for the platform's next iteration.

### 8.6.6 Net Promoter Score

Ten respondents answered the NPS question. Promoters numbered 5 (50 %), passives 4 (40 %) and one detractor (10 %). The resulting Net Promoter Score was 40, a generally favourable result (scores above ~20 are positive). In disaggregated analyses, researchers' NPS was 80 (four promoters, one passive) while participants' NPS was 40 (two promoters, three passives). Open-ended remarks echoed CSAT themes, highlighting secure study management, a centralized space for informed consent and an intuitive interface; suggestions for improvement focused on clearer help/error messages, stronger filtering and navigation, dashboard customization, and a dark mode.

*Table 18 - Net Promoter Score survey results.*

| Category | Count | % |
|---|---|---|
| Promoter (9–10) | 5 | 50.0 |
| Passive (7–8) | 4 | 40.0 |
| Detractor (0–6) | 1 | 10.0 |

## 8.7 Discussion

The discussion interprets the empirical signals from the usability, skills, self-efficacy, satisfaction, and loyalty measures in light of the platform's design goals and the broader literature on dynamic informed consent. Adopting the thesis's critical-realist stance, it considers how observed patterns arise jointly from system properties and user characteristics. Subsections address (i) overall usability and user satisfaction, (ii) digital-ability and self-efficacy profiles and their implications for support and onboarding, (iii) loyalty and advocacy as indicated by NPS, (iv) sample composition and measurement limitations, and (v) concrete design and research directions. The aim is to translate descriptive results into actionable guidance for the Consentio roadmap while remaining analytically modest about scope and generalizability.

### 8.7.1 Addressing Section 8's Research Questions

Section 8 synthesizes quantitative survey data, task observations, and an examination of the Consentio platform's architecture to answer the overarching research question: How do dynamic informed-consent features and blockchain-based audit capabilities within Consentio shape users' trust, perceived usability and motivation to participate in public health research? To provide a more granular analysis, the question is divided into three subquestions:

- RQ1. To what extent does Consentio reduce perceived effort and coordination overhead for study setup and management?
- RQ2. How do dynamic-consent features and user experience affect participants' willingness to enroll in public-health studies?
- RQ3. How does the use of blockchain empower consent processes and give users control over their data?

The discussion below draws on findings from the updated surveys (usability, digital skills, self-efficacy, customer satisfaction, Net Promoter Score and demographics), task observations, and the rationale outlined in Sections 6 and 7 to address each sub-question. Chapter 9 then examines the interview and open-ended responses that explain how participants made sense of control, transparency, usability, and trust.

### 8.7.2 [RQ1] - Enhancing the Ease of Publishing and Managing Research

Across our hybrid sessions (n=10; five researchers, five participants), centralizing study creation, dynamic consent, participant status, and dissemination within a single dashboard reduced coordination overhead and made permission states auditable, echoing Theme 1 ("confidence in data management"). Ceiling-level ISS operational skills (≈5.0) and strong information navigation (≈4.25) aligned with uniformly high satisfaction and perceived ease of use, while interviews described tangible productivity gains from immutable, role-segregated records. Technically, the Fabric-based ledger, smartcontract guards and segregated researcher/participant views operationalized governance requirements and were reflected in a high usability

score (M = 1.82, SD = 0.45 on the reversed scale; 95 % CI = 1.50–2.14). Improvement priorities still converge on progressive disclosure, clearer status indicators and responsiveness tuning, given the higher mean on the recoveryfromerrors item. These refinements are incremental because the core usability remains strong. Consistent with the RQ summary, improvement priorities converge on progressive disclosure, clearer status indicators, and responsiveness tuning, given lower scores on error/help clarity and qualitative notes about latency and navigation. With Consentio's modular architecture, these refinements are incremental; forthcoming smart systems integration(SSI), integration is expected to further streamline preference portability across studies and institutions.

### 8.7.3 [RQ2] - Participants' Willingness to Enroll in Public Health Studies

Willingness to participate tracked trust, perceived value and interaction ease. The combined Net Promoter Score was 40, derived from 5 promoters, 4 passives and 1 detractor. Researchers' NPS was 80 (four promoters, one passive), while participants' NPS was 40 (two promoters, three passives). All respondents were satisfied or very satisfied with the platform and intended to continue using it. Interviews linked this comfort to monitoring consent status, managing participation and seeing results in one place; many participants explicitly connected granular, real-time control to greater willingness to enrol. Interviews linked comfort to monitoring consent status, managing participation, and seeing results in one place; 71% explicitly tied granular, real-time control to greater willingness (Theme 4), and those expressing confidence in data management tended to rate PSSUQ items highly. At the same time, our small, young, highly educated sample (ISS ≈3.75/5; CUSE ≈2.96/6) indicates that users with lower self-efficacy may require more guidance. Integrating the RQ summary's design priorities, deployments should include summarized consent views, accessible language, guided tutorials, optional low-tech supports, and competence-adaptive interfaces so that dynamic consent remains empowering rather than intimidating.

### 8.7.4 [RQ3] - Blockchain's Role in Empowering Consent and Data Control

The permissioned ledger contributed tamper-evident stamping, strict time-ordering, and policy-enforcing contracts, producing a verifiable audit trail beyond the control of any single actor; 71% of participants cited

this auditability as trust-enhancing in debriefing comments, a point examined qualitatively in Chapter 9. Coupled with dynamic consent, ledgered events enabled rapid propagation of revocations and transparent histories, reinforcing a sense of procedural fairness. Interviews, however, revealed confusion about the fate of previously collected data after withdrawal (delete vs. retain vs. restrict), underscoring the RQ-summary recommendation to communicate the data life cycle explicitly and to surface post-revocation states in plain language. Leveraging Fabric private channels and off-chain storage anchored by on-chain hashes supports data minimization and sovereignty; documenting these choices, clarifying sustainability considerations, and refining help/error messaging are pragmatic steps to consolidate perceived integrity and user control.

### 8.7.5 Implications for Design and Future Research

The survey results identify usability, satisfaction, and self-efficacy patterns; the next chapter examines the interview and open-ended responses that explain how participants made sense of control, transparency, and trust.

Findings affirm strong core usability and high satisfaction/loyalty among digitally literate users, while pointing to focused improvements: clarify recovery and help states (as indicated by the PSSUQ Q9 signal), reduce cognitive load through progressive disclosure in consent flows, enhance filtering and navigation responsiveness, and offer dark mode and dashboard personalization. Pair these with lightweight, just-in-time tutorials for advanced tasks surfaced by ISS/CUSE gaps. To broaden accessibility, expand testing across diverse ages, abilities, and skill levels, conduct accessibility audits aligned with WCAG 2.1 (Andrew Kirkpatrick et al., 2025), and experiment with interfaces that adapt the level of explanation to users' competence. Longitudinally, repeat surveys and segment NPS by role to track whether design changes move usability, satisfaction, and advocacy in the intended directions. Finally, document and communicate the platform’s environmental footprint and the post-revocation data lifecycle to address sustainability and data-handling concerns without diluting the security/audit guarantees that users already value.

## 8.8 Conclusion

This section presented a mixed-methods evaluation of Consentio, combining standardized instruments and targeted questionnaires to assess usability, digital skills and self-efficacy, customer satisfaction, loyalty and respondent characteristics. The Post-Study System Usability Questionnaire indicated strong perceived usability, with consistently low item means and a global score of 1.82 (SD = 0.45; 95% CI = 1.50–2.14) on the 1–7 response scale where lower values reflect more favourable perceptions; item-level patterns suggest that routine workflows and navigation were experienced as straightforward, while recovery from errors remained the clearest area for improvement. Complementing this, the Internet Skills Scale and the Computer User Self-Efficacy results showed high operational and mobile competence alongside greater variability in information navigation and reduced confidence in advanced or creative tasks, implying that future iterations should pair strong core interaction design with clearer help content and lightweight onboarding to support less confident users.

Customer satisfaction responses were uniformly positive across the closed-ended CSAT items, and loyalty intent was similarly strong: across all respondents, the Net Promoter Score was 60, with promoters outnumbering passives and no detractors. Taken together, these findings support the claim that Consentio meets its usability objectives for this sample and that users perceive sufficient value and trust to recommend the platform. At the same time, the small and relatively homogeneous sample constrains external validity; the results should therefore be read as formative evidence that motivates targeted refinements (notably around error recovery and support information) and justifies broader, more diverse field evaluations to test robustness, equity of use, and longitudinal dynamics under realistic research conditions.

Because the evaluation involved ten participants, the quantitative results should be interpreted as exploratory usability evidence rather than population-level estimates. The sample is appropriate for identifying interface issues, surfacing design implications, and testing whether the governance-to-platform translation is understandable to early users, but it cannot establish statistical generalizability, subgroup effects, or stable estimates of acceptance across public-health research populations.

# 9 Reflexive Thematic Analysis of Consentio Dynamic Informed Consent Platform Based on Participants' Interviews and Surveys' Discursive Answers

## 9.1 Introduction

Digital platforms for dynamic consent promise to transform how researchers and research participants negotiate the terms of data sharing. Consentio is one such platform that offers a unified environment for managing consent, tracking study enrolment and withdrawal, and presenting audit trails through a private ledger. Quantitative metrics, such as usability scales and satisfaction scores, offer important signals, yet they do not capture the nuance of how human actors understand an (Ahmed et al., 2025; Anderson et al., 2016; Braun & Clarke, 2006; Spencer et al., 2016; Wallace & Miola, 2021)l., 2016; Wallace & Miola, 2021). This section integrates qualitative analysis of semi-structured interviews (Asklund et al., 2019; Dobson et al., 2023; Drogt et al., 2022; Mannonen et al., 2014), based on open-ended feedback from researchers (R1 – R5) and data subjects (P1–P3) who evaluated the platform. Reflexive Thematic Analysis (RTA) (Braun et al., 2022; Braun & Clarke, 2019, 2021, 2024a; Campbell et al., 2021), is used to synthesize these data. By bringing researcher and participant perspectives into dialogue, the section builds a holistic picture of Consentio's strengths, limitations and future design needs.

## 9.2 Epistemic Stance and Methodology

The following sections present the epistemic stance and the methods used to conduct the thematic analysis of the interviews. This aims to provide readers with an honest and ethical assessment of the author's epistemological orientation, the methods used and guided by that orientation, the data and instruments, the effects (e.g., questionnaire domain), and the reflexive nature of the thematic analysis (McNamara, 2013).

### 9.2.1 Epistemic Stance

To conduct the thematic analysis of the interview transcripts, we decided to present our epistemic stance to readers, making clear the epistemological orientation that guided the methods and conclusions. The motivation for this approach stems from the author's training in quantitative methodologies, given the nature of their academic career. However, with the requirements needed to complete a qualitative assessment of the interviews, it is possible to provide more complete results from participants' user experience with the platform. In (Poole et al., 2019), the authors noted that, over time, the use of epistemic stance indexes increases, whilst indexes of doubt or uncertainty decrease. In fact, their study presented a Kendall's Tau analysis of modal auxiliaries (e.g., can, will, may, must, could, might, would, should), adoption in scientific writing with a clear increase in more confidence representing one, such as '*can*' and "*will*"; And an reduction in use of auxiliaries that represents more doubt or uncertain one, such as "*might*" and "*would*".

Communicating a truthful and reliable thematic analysis is the goal of this section, so constructing an epistemic stance that reflects accurate auxiliaries and hedges (Poole et al., 2019), is of critical importance to provide readers with the means to assess fairly the methodology applied and the results presented. For that reason, we grounded our analysis in critical realism, which assumes that phenomena relevant to dynamic informed consent, ledger technologies, and data governance exist independently of our analysis (McNamara, 2013; Roseano et al., 2016). The themes mapped were derived from recurrent patterns identified in the interviews, not as a hidden truth to be found; thus, they should not be accepted as all the possible themes one could extract. The below shows some excerpts from the interviews.

*Table 19 - Recurrent excerpts used for theme mapping.*

| Theme | Excerpt | Source |
|---|---|---|
| Data Control with Caveats | "*I've participated in other studies… my data already exists somewhere else. I don't know what's happening with that data… how I could get that data back or wipe it from the internet.*" | P1, p0001.docx, ~00:00:38–00:01:20 |
| | "*I'd be more inclined to participate knowing there's something that controls my data privacy… I feel like I have more control over how it's shared.*" | P3, p0003.docx, ~00:08:10–00:08:49 |
| Transparency That Is Explained, Not Assumed | "I'm not a blockchain expert… it needs to be explained more clearly how it works and why it's more secure." | P1, p0001.docx, ~00:02:00–00:02:16 |
| | "*Knowing there's a record of actions with exact timestamps, and that users can't delete them, makes it clear things are properly maintained*." | P2, p0002.docx, ~00:01:24–00:02:24 |
| Usability That Protects Informedness | "*There were buttons where I could skip ahead… but if someone skips without reading, is it still informed consent?*" | P2, p0002.docx, ~00:02:53–00:03:55 |
| | "*It's straightforward… a lot of information to digest, which is understandable*." | P1, p0001.docx, ~00:04:21–00:04:41 |
| Motivation Sustained by Centralisation and Feedback | "*Often you never hear about the study again… a platform where you could log in a year later and see a link to the paper would keep people engaged.*" | P1, p0001.docx, ~00:06:06–00:07:10 |
| | "*Being able to go behind a screen and say 'I don't want my data to be part of the study anymore' allows actual consent with no pressure.*" | P2, p0002.docx, ~00:05:20–00:06:34 |
| Usability and User Interface Experience (Researchers) | "*Minor UI issues… e.g., start/stop buttons, and not being able to click the survey name, had to go to the right and click manage actions*." | Researcher G, Interview Transcripts (PDF), ~1:03:20 |
| | "*Compared to similar academic software like REDCap… this felt accessible; actions make sense and it's easy to find what you want.*" | Researcher G, Interview Transcripts (PDF), ~1:08:28–1:09:05 |
| Centralised Study Management and Participant Tracking (Researchers) | "*Very useful to have everything in one place… current consent processes are email/document-based and detached from data collection and compliance.*" | Researcher G, Interview Transcripts (PDF), ~1:01:56–1:03:07 |
| | "*Study management and dynamic consent management… helpful to manage our study.*" | Researcher J, Interview Transcripts (PDF), ~38:21–38:53 |
| Customisation and Personalisation (Researchers) | "*If a new person is creating a study, adding more Help/support, little symbols by fields that say what we expect in this field, would be good.*" | Researcher J, Interview Transcripts (PDF), ~39:21–39:27 |
| | "*Within each tab… add more information on how it has to be used; initial steps and Help resources were useful.*" | Researcher J, Interview Transcripts (PDF), ~42:48–43:19 |
| Communication and Notification Preferences & Data Presentation (Researchers) | "*The chat feature was helpful… an opportunity to chat with participants to get queries about the studies.*" | Researcher J, Interview Transcripts (PDF), ~38:21–38:53 |
| | "*At a glance, see how many have been contacted, how many consented, how many had data collected, that's something I'd look for.*" | Researcher G, Interview Transcripts (PDF), ~1:11:13–1:11:32 |

## 9.3 Reflexive Thematic Analysis

Both analyses employed Reflexive Thematic Analysis (RTA) as theorized by (Braun & Clarke, 2024a), a flexible, interpretivist technique oriented to identifying patterns of shared meaning underpinned by a central organizing concept. RTA treats themes as interpretive constructs rather than frequency counts; researcher subjectivity is considered a resource rather than a threat. The analysis unfolded through six iterative phases: (1) familiarization with transcripts and open-ended comments; (2) initial coding at sentence or clause level; (3) generation of candidate themes; (4) review of themes for internal coherence and external distinction; (5) definition and naming of themes; and (6) production of a narrative report. Reflexive memos, codebooks and decision logs were maintained to ensure an auditable trail.

Additional details about each phase underscore the reflexive and iterative nature of RTA. In the familiarization phase, the analyst immersed themselves in the data by reading each transcript and surveying comments multiple times while making reflective memos. These memos captured initial impressions, questions, and positionality statements, acknowledging how the analyst's disciplinary background and values might shape coding decisions. Initial coding proceeded at the sentence or clause level using semantic codes (capturing explicit meanings) and, where appropriate, latent codes (inferring underlying assumptions). Codes were short descriptors that stayed close to the participant's language; they were continually refined as new insights emerged (Braun et al., 2022; Braun & Clarke, 2006).

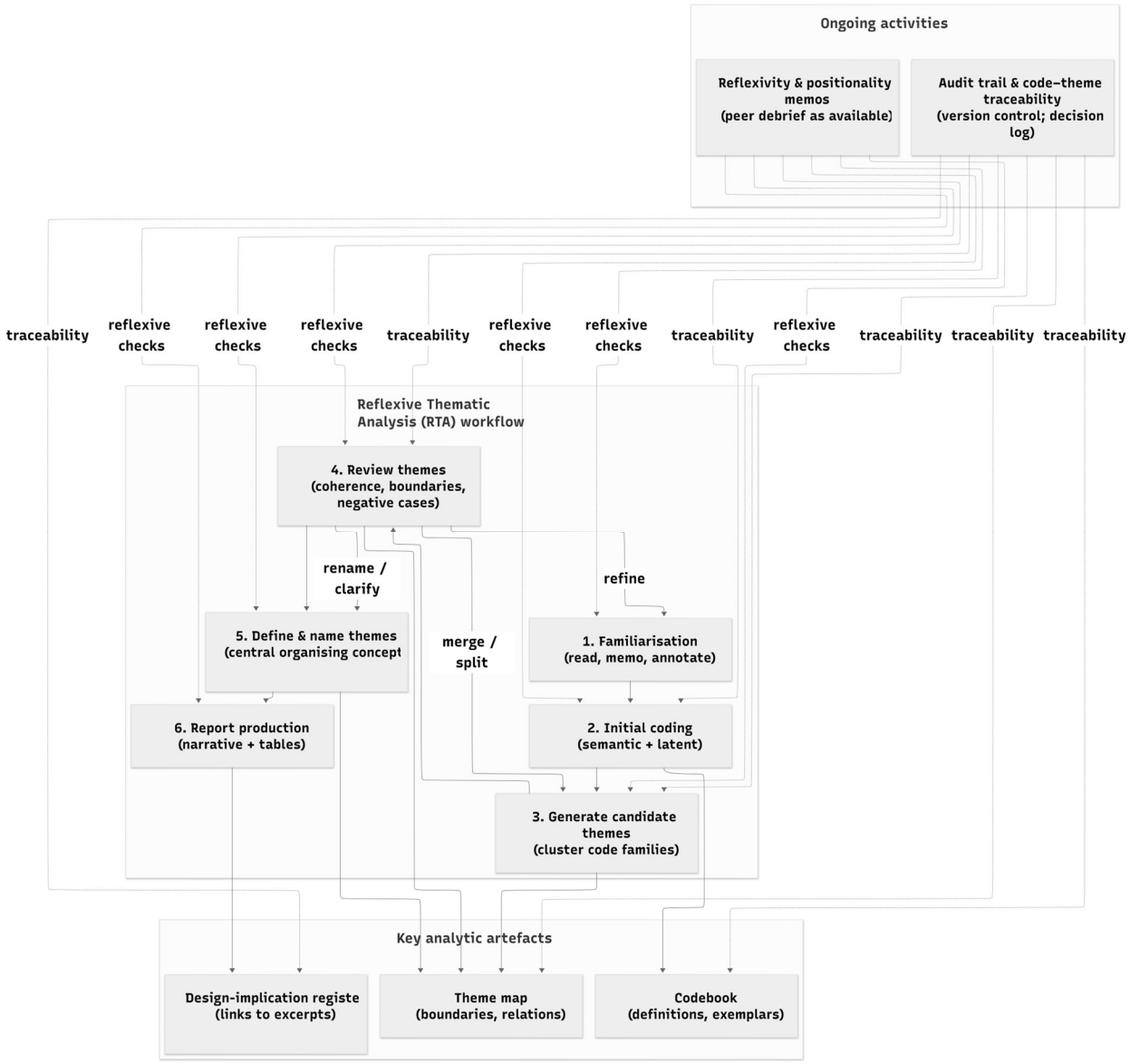
Once a substantial code set had been created, codes were clustered into candidate themes by examining relationships and shared meanings. This clustering was not mechanical; it involved constant comparison across codes and an openness to multiple interpretations. Candidate themes were then subject to a review process in which their coherence and distinctiveness were tested against the entire data set. This step often led to collapsing overlapping themes, splitting broad ones, or redefining boundaries. Negative case instances that contradicted the emerging narrative were deliberately sought to challenge early assumptions and refine thematic boundaries (Braun & Clarke, 2022). In the definition and naming phase, themes were articulated as concise statements centred on a unifying concept; inclusion and exclusion

criteria were written down; and exemplary extracts were selected to illustrate each theme. A detailed codebook and theme map were produced as key analytic artifacts, documenting definitions, exemplary excerpts and the relationships among themes. The theme map served as a visual representation of how themes connect and build on one another, while the codebook ensured traceability from raw data to thematic interpretations.

Finally, the report production phase involved crafting a narrative that explains how the themes answer the research questions and interact with one another. Throughout all stages, reflexivity and positionality memos were revisited to ensure that interpretations remained grounded yet self-aware. An audit trail, comprising version-controlled codebooks, decision logs and annotated transcripts, was maintained, supporting transparency and enabling others to follow the analytic process (Braun et al., 2022).

Figure 15 below summarizes the RTA workflow, highlighting the six phases, the ongoing activities (reflexivity and audit trail) and the key analytic artifacts produced at each stage.

*Figure 15 - Reflexive Thematic Analysis workflow diagram.*




## 9.4 Interviews and Data Sources

This section describes the participants and data sources used for the thematic analysis. Both data subjects and researchers had unique questionnaires tailored to their point of view regarding the platform (Brinkmann, 2015a, 2015b). The data subjects' questionnaire had open-ended questions that tried to assess their experience with browsing available studies, granting or revoking consent to public health studies and their feelings about the underlying blockchain layer for storing consent history. For researchers, the

questionnaires focused on the processes involved in creating studies, submitting studies for approval, revising data auditors and principal investigators' revisions, and finally publishing the study for data subject users of the platform to have access to its details and opting out via dynamic consent functions. It also had questions regarding the platform's functionalities to manage studies, such as start, pause, stop and end a study; The options to manage participants, such as requesting reconsent, answering questions via the chat page, and sending messages to all participants at once. Finally, the researcher dashboard with statistics visualization regarding different metrics of their studies, such as the number of participants, the number of withdrawals, the number of studies wishlisted, the number of studies ongoing, pending approvals, and historical enrollments and withdrawal metrics (DeJonckheere & Vaughn, 2019; Guest et al., 2006; Turner, 2010). Both questionnaires are available in Appendix A and B.

### 9.4.1 Data Subjects and Researcher Interviews

Two cohorts took part in the qualitative study: data subjects (n = 5; P1–P5) and public-health researchers (n = 5; R1–R5). Both cohorts completed semi-structured interviews tailored to their role but aligned on common analytic domains. Demographic survey data indicate that half of the respondents resided in Canada (5/10, 50%), 40% were aged 25–34 (4/10), and 10% were 18–24 (1/10), with the remainder not reported. Forty percent identified as women (4/10) and 10% as men (1/10). Regarding occupation, 40% were students (4/10) and 10% were employed full-time (1/10). Educational attainment skewed high: 30% reported a postgraduate degree (3/10) and 10% a PhD (1/10), with additional responses including college graduate (10%), some college (10%), and other (10%). Self-rated technical proficiency clustered at advanced (30%) and expert (10%), with 10% intermediate. Prior experience with electronic health records or patient portals was common (50% "yes," 10% "no," 40% not reported). Study awareness was primarily via word of mouth (40%), with 10% via social media(Kallio et al., 2016).

For data subjects, the guide covered data control, transparency and trust, usability and user experience, and motivation to participate. For researchers, prompts targeted platform utility for research workflows, trust in a private-ledger/permissioned-blockchain backbone, dynamic-consent management,

tech-savviness and usability, and suggestions for improvement. Interviews were audio-recorded, transcribed verbatim, anonymized, and analysed in two parallel streams using Reflexive Thematic Analysis (RTA), one for data-subject interviews and one for researcher interviews, to preserve role-specific standpoints while enabling cross-role comparison. Illustrative extracts are quoted verbatim (lightly edited for readability) with identifiers P# for data subjects and R# for researchers; when relevant, we also point to comments originating from survey free-text responses (Brinkmann, 2015a; Kallio et al., 2016).

*Table 20 - Participants' demographics.*

| Characteristic | Category | Count (N=10) | Percentage |
|---|---|---|---|
| Age | 18–24 years | 1 | 10% |
| | 25–34 years | 4 | 40% |
| | Not reported | 5 | 50% |
| Gender | Man | 1 | 10% |
| | Woman | 4 | 40% |
| | Not reported | 5 | 50% |
| Occupation | Employed (full-time) | 1 | 10% |
| | Student | 4 | 40% |
| | Not reported | 5 | 50% |
| Highest Qualification | College Graduate | 1 | 10% |
| | PhD | 1 | 10% |
| | Postgraduate Degree | 3 | 30% |
| | Some College | 1 | 10% |
| | Other | 1 | 10% |
| | Not reported | 3 | 30% |
| Technical Proficiency | Advanced | 3 | 30% |
| | Expert | 1 | 10% |
| | Intermediate | 1 | 10% |
| | Not reported | 5 | 50% |
| Residency | Canada | 5 | 50% |
| | Non-Canada | 5 | 50% |
| Prior EHR Experience | No | 1 | 10% |
| | Yes | 5 | 50% |
| | Not reported | 4 | 40% |
| Study Awareness Source | Social Media | 1 | 10% |
| | Word of Mouth | 4 | 40% |
| | Not reported | 5 | 50% |

### 9.4.2 Surveys and Questionnaire Feedback

All participants, data subjects and researchers completed the same post-use survey battery, comprising the Post-Study System Usability Questionnaire (PSSUQ) (Will, 2026), a satisfaction survey, a Net Promoter Score (NPS) item (Fisher & Kordupleski, 2019; Nadanyiova et al., 2022), and a demographic questionnaire.

Open-ended responses from these instruments were compiled for both cohorts and analysed qualitatively using RTA to contextualize the quantitative scores and to surface latent needs (e.g., requests for filtering, dashboards, audit-receipt visibility, and clearer withdrawal outcomes). The study also deployed the Internet Skills Scale (ISS) (Jurkovic & Kopal, 2025; van Deursen et al., 2016) and the Computer User Self-Efficacy (CUSE) (Cassidy & Eachus, 2002) scale to gauge digital ability. Participants rated system usefulness and interface quality highly, with 98.6 % of PSSUQ responses indicating agreement or strong agreement. ISS responses showed that 64 % of ratings were "very true," suggesting strong operational and information skills, while the CUSE distribution was bimodal: 26 % responded "5" and 25 % responded "1," indicating both high and low self-efficacy co-existing within the sample. In the NPS survey, 50 % of respondents were promoters (rating 9–10), 40 % were passives (rating 7–8), and 10 % were detractors (rating 0–6). The overall Net Promoter Score was 40, which is favourable given the small sample size; nonetheless, all respondents were at least "likely" to recommend the platform. When we cite survey comments directly, the same attribution convention (P# or R#) is used to signal the respondent's role.

## 9.5 Research Questions Strategies

This section employs Reflexive Thematic Analysis to examine how Consentio's affordances are interpreted in practice, prioritizing meaning and mechanism over magnitude. We analyse semi-structured interviews with researchers and participants alongside discursive survey responses, adopting a critical realist stance in which themes are analytically constructed as models of patterned accounts. The aim is to surface how control, transparency, usability, and motivation are experienced, the conditions under which they succeed or fail, and the trade-offs users articulate as they navigate consent decisions.

### 9.5.1 RQ1 — How Do Users Understand and Exercise Control Over Their Personal Data When Using Consentio?

Users' understanding and exercise of control over their personal data emerged as a central dimension of Consentio's value proposition, but this control was not interpreted as absolute or unlimited. The analysis

drew on participant interviews, researcher interviews, and open-ended survey responses addressing withdrawal, consent-status indicators, action receipts, consent history, and perceived limits on downstream data use. Across these accounts, participants appeared to value the ability to grant, revise, and withdraw permissions within a centralized platform because these actions made consent visible, actionable, and revisable over time. However, users also recognized that withdrawal may not fully reverse all prior data movements, particularly where data had already been exported, aggregated, analyzed, or incorporated into published outputs. Therefore, control was best understood as situated and temporally bounded: Consentio strengthened participants' ability to govern future access and understand current permission states, but it also needed to communicate the practical and legal limits of revocation after data had moved beyond the immediate platform environment.

Analytically, this research question was addressed through reflexive coding of interview narratives and open-ended survey text for accounts of granting consent, changing permissions, withdrawing participation, interpreting provenance, and understanding downstream data-use consequences. The interpretation distinguished evidence of meaningful control, such as clear options, reversible actions, legible outcomes, and proof-of-action receipts, from more nominal forms of control, where interface states were confusing, consequences were unclear, or revocation was perceived as technically or institutionally limited. Participant and researcher perspectives were compared to identify convergences and tensions, including cases where researchers viewed the platform as an improvement in consent governance while participants still requested clearer explanations of what withdrawal could and could not accomplish. The implication for Consentio is that participant control should be materialized through visible action receipts, status badges, consent-history views, and revocation-outcome panels that explain, in plain language, whether data collection has stopped, whether custodians have been notified, whether previous exports are affected, and whether already aggregated or published results remain outside the scope of withdrawal.

### 9.5.2 RQ2 — What Signals and Explanations (In the Interface or Process) Foster Transparency and Trust Among Users?

Transparency and trust were not produced by the existence of ledger technology alone, but by the extent to which the platform translated auditability into evidence that users could understand. The data used to answer this question included comments about ledger receipts, consent history, study information, notifications, audit trails, and explanations of data handling. Participants and researchers tended to associate trust with visible records of action, clear study information, and the ability to verify what had happened to consent decisions over time. However, the analysis also suggested that technical assurances could remain abstract or inaccessible when users did not understand how blockchain, private ledgers, role-based access, or immutable records related to their own rights and decisions. Thus, trust was fostered when the interface explained not only that an event had been recorded, but what the event meant, who acted, what data or permission state was affected, and what options remained available to the participant.

The analytic focus for this question was on episodes where explanations clarified or obscured governance and audit guarantees. Interview and survey material was coded for references to timing, wording, modality, confirmations, consent-history visibility, and perceptions of the ledger as either reassuring or opaque. The interpretation criteria emphasized movement from technical assurance to experienced assurance: users needed to feel that they knew what happened, who could see or act on their data, why a state had changed, and what would happen next. Trust was threatened when explanations were too technical, when governance processes were hidden behind generic confirmations, when notification language lacked consequence, or when users' mental models did not match the platform's actual data-handling workflow. The resulting design implication is that Consentio should pair ledger-backed events with plain-language receipts, role-and-access summaries, stepwise disclosures, and study-specific audit explanations. In this way, transparency becomes a user-facing governance practice rather than a background technical property.

### 9.5.3 RQ3 — Which Aspects of the Platform's Usability Support or Threaten the Principles of Informed Consent?

The analysis indicated that usability should be treated as an ethical condition of informed consent rather than as a secondary matter of interface polish. This research question drew on task observations, PSSUQ, CUSE, CSAT, and NPS patterns, as well as interview comments regarding navigation, form length, terminology, skip-ahead behavior, information density, and user confidence. Consentio's usability supported informed consent when it helped participants understand the study, review relevant risks and data-use conditions, revisit decisions, and act without unnecessary friction. Features such as progressive disclosure, recap screens, consent history, just-in-time definitions, predictable controls, and reversible actions appeared to scaffold informedness by reducing cognitive burden while preserving participant agency. Conversely, usability threatened informed consent when interface efficiency risked becoming premature consent, such as when participants could move too quickly through essential information, when labels were ambiguous, or when information volume became overwhelming.

The analytic approach involved a close reading of consent flows triangulated with participants' and researchers' accounts of friction, fluency, confusion, and confidence. The key interpretive criterion was whether the platform enabled accurate, effort-proportionate understanding at the point of decision. This meant asking whether users could reasonably understand what they were agreeing to, what data would be used, who would access it, how long the permission would remain active, and how they could later modify or withdraw that decision. Breakdowns were mapped to specific interface and content patterns, including unclear terminology, excessive text density, inconsistent controls, insufficient recovery states, and shortcuts that might weaken comprehension. The implication is that Consentio should treat progressive disclosure, confirmation recaps, glossary support, predictable navigation, accessibility patterns, and recovery/help states as governance requirements. Informed consent depends not only on the presence of information, but on whether the interface makes that information usable at the moment when participants are asked to make a consequential decision.

### 9.5.4 RQ4 — What Factors Motivate or Discourage Continued Participant Engagement in Public-Health Research When a Dynamic Consent Platform Is Used?

Continued engagement with public-health research appeared to depend on whether Consentio could transform participation from a one-time enrollment event into an ongoing, meaningful relationship between participants and research activity. The data used to answer this question included participant and researcher interviews, open-ended survey responses, and comments about dashboards, study-status visibility, feedback on outcomes, reminders, alerts, notifications, and support. Participants were more likely to view ongoing participation positively when the platform provided a central study hub where they could see active and past studies, track consent status, receive notifications about term changes, and access information about study results or publications. Researchers similarly valued centralized study management because it reduced administrative burden and created clearer channels for participant tracking, re-consent, messaging, and follow-up. Engagement, therefore, was motivated by perceived value, visibility, reciprocity, and confidence that participation remained under the participant's control.

At the same time, the analysis showed that engagement could be discouraged by notification fatigue, unclear status information, uncertainty about long-term data handling, insufficient feedback about study outcomes, or lack of accessible human support when questions arose. The analytic approach contrasted researcher and participant perspectives on why users might stay engaged, disengage, withdraw, or ignore platform communications. These accounts were then linked to concrete touchpoints in the platform, including dashboards, alerts, consent-history views, re-consent requests, chat functions, and study-result feedback mechanisms. The interpretation criteria focused on identifying coherent mechanisms connecting features to sustained engagement or attrition, while also considering boundary conditions such as digital ability, prior research experience, trust in institutions, and comfort with health-data technologies. The implication is that Consentio should strengthen continued engagement through a central "My Studies" hub, clear term-change alerts, outcome feedback, accessible support, and notification practices that respect autonomy, cognitive load, and participant time. In this model, engagement is not achieved through more

frequent communication alone, but through communication that is timely, meaningful, actionable, and visibly connected to participants' rights and contributions.

## 9.6 Analytic Orientation and Quality Procedures

The analysis adopted a pragmatic-constructivist epistemology (McNamara, 2013; Roseano et al., 2016). Participants' utterances were treated as situated sense-making about concrete interface encounters and normative expectations in a public-health context. Coding privileged semantic meaning but remained open to latent meanings where interviewees invoked implicit premises, such as the tension between immediate revocation and the practical impossibility of recalling exported data. To enhance credibility, thick descriptions and negative cases were preserved; dependability was strengthened through dated memos and version-controlled notes; confirmability was addressed by explicitly acknowledging the analyst's positionality and assumptions. Given the small purposive sample, transferability is limited, yet contextual detail and analytic transparency support readers in judging relevance to other settings.

## 9.7 Results: Themes Across Participants and Researchers

The analysis yielded eight overarching themes synthesized across the participant interviews and researcher feedback. Four of these themes derived primarily from participant accounts and probe how end-users understand control, trust, usability and motivation. The remaining four themes emerged from researcher feedback and focus on practical aspects of platform design, usability, centralization of study management, customization, and communication/data presentation. Where appropriate, themes are integrated to illuminate commonalities and divergences.

In an extended analysis, codes from interviews were crosslinked with survey responses to quantify theme salience. All seven interviewees referenced confidence in data management, five discussed transparency and trust, six commented on usability and experience, five noted the impact on willingness to participate, and six highlighted challenges and improvements. These frequencies align with the high

proportions of positive PSSUQ and ISS responses indicate that participants who valued the platform's audit trail and centralized dashboard were also more likely to be satisfied overall.

### 9.7.1 Theme 01: Data Control with Caveats

This theme captures participants' appreciation for the platform's central promise, being able to manage consent centrally and withdraw at will, while acknowledging uncertainties about data that have already left the platform. Participants celebrated the opportunity to stop future access yet recognized that exported data cannot be fully retracted. They called for clear boundaries around revocation and a visible locus where they could enact control (e.g., enroll, pause or withdraw) and verify the outcome.

Illustrative Excerpts – P1 reflected that although Consentio secures data "*from that point on*," their data already exists in other platforms; they are unsure "*how I could…wipe it from the internet*" to ensure the only copy resides on Consentio. P2 appreciated that the platform makes it "*easier to manage which studies you are part of*", highlighting the value of a central hub. P3 described how consent forms "*get misplaced*" in paper-based processes and praised the ability to withdraw and receive notifications of updates, noting that "*if there's an update to [the] study, you get a notification*". A researcher similarly emphasized the need for revocation clarity, asking for a "*Revocation Outcomes panel per study*" that explains whether prior exports must be deleted and whether published analyses remain.

Subthemes and Design Implications – Table 21 summarizes the subthemes: (a) Revocation clarity vs. downstream copies, participants want reassurance that stopping future access is possible while recognizing the limits on retrieving already exported data; (b) Scope boundaries, they ask which data elements are subject to revocation (API cut-off, visibility change, lawful retention exceptions); and (c) Actionability locus, they request clear buttons to enrol, pause and withdraw, accompanied by status badges and receipts. Responding to these needs, researchers proposed a Revocation Outcomes panel and highlighted the importance of surfacing export controls at consent time.

### 9.7.2 Theme 02: Transparency That Is Explained, Not Assumed

Participants and researchers converged on the idea that transparency is not achieved merely by deploying private ledger technology; it requires human-readable explanations. Audit trails, cryptographic mechanisms and permissioned ledgers inspire confidence only when their purpose and operation are made explicit. Without translation, the ledger can become "*background magic"*.

Illustrative Excerpts – P1 admitted to being "*not a blockchain expert*" stressing that :"*for the average person it needs to be explained a little bit more clearly how the blockchain works and why it's more secure*". P2, who has basic knowledge of blockchain, valued the immutable action history, ",*knowing that even if you click a particular button, that will show up in the record of actions with the exact timestamp*". However, P2 noted that this transparency is only meaningful if users understand what is being recorded and for what purpose. Researchers echoed these sentiments: they found auditability reassuring but asked for "*plain-language security*" that translates ledger jargon into human meaning, including tables detailing who can access which data, under what legal basis and for how long. One researcher suggested a concise "Why your data is safe here" explainer accompanied by diagrams and cross-links to the audit log.

Subthemes and Design Implication – Subthemes include: (a) Auditability reassures, timestamped consent logs and verifiable receipts provide accountability; (b) Plain-language security, users need explanations of tamper-evidence, role-based access and the consequences of withdrawal; and (c) Access tables, presenting actors, data items, legal bases and durations, fosters trust. The design implications point toward creating human-readable security explainers, adding an access table on each study page and integrating diagrams that link the ledger to real-world protections.

### 9.7.3 Theme 03 – Usability That Protects Informedness

Participants emphasized that the flow is straightforward and efficient but warned that shortcuts, such as skip-ahead buttons, could erode informed consent if not carefully regulated. Researchers similarly valued ease of navigation but noted minor inconsistencies between interface behaviour and user expectations (e.g.,

clickable names vs. separate management buttons). Both groups agreed that progressive disclosure, clear navigation and consistent controls minimize friction while preserving comprehension.

Illustrative Excerpts – P2 enjoyed that they did not "*have to click through the whole thing again*" when revisiting sections, but cautioned that unrestrained skip-ahead could compromise informedness: "*if a person doesn't go through the whole thing … and they skip ahead to enroll without reading, is it still informed consent?*". P3 affirmed that the interface was "*very helpful*" compared to paper forms, yet emphasized that participants still need to understand "*what you just agreed to*" From the researcher surveys, respondents described the interface as "*easy*" or "*very easy*" to navigate but noted minor conflicts, such as "*not being able to click survey names*" which can disrupt the experience.

Subthemes and Design Implications – Table 22 lists subthemes: (a) Progressive disclosure, accordion summaries and expandable details help manage cognitive load; (b) Skip-ahead tension, balancing convenience against comprehension; (c) Consistent controls, ensuring clickable elements behave as expected; and (d) Confirmation recap, providing a short summary of key points before finalizing consent. Design recommendations include gating enrolment behind brief acknowledgements of key points, adding just-in-time definitions, and offering a confirmation screen that recaps the user's choices. Researchers proposed that skip-ahead should be available only after a full viewing on the first visit, preventing uninformed consent.

### 9.7.4 Theme 04: Motivation Sustained by Centralization and Feedback

Participants linked their willingness to participate in research not only to control and trust but also to tangible benefits, such as a single hub to manage studies and feedback on research outcomes. Having all enrolments, statuses and histories in one place reduces cognitive load and fosters engagement. Visible feedback loops, such as links to publications or lay summaries, validate participation and encourage continued involvement. Researchers also valued centralization for administrative efficiency and suggested features that support communication and monitoring.

Illustrative Excerpts – P2 appreciated that Consentio helps them "*find out which studies you might be able to participate in*" and keeps track of past and upcoming studies. P1 argued that a centralized platform could allow participants to log in "*a year later and see a link to the paper that was published based on their participation,*" which could "*keep people more engaged*". Researchers likewise highlighted the benefits of "*a unified location to keep track of all research studies and to get updates*" emphasizing that centralized management reduces administrative burden and memory lapses.

Subthemes and Design Implications – Subthemes include: (a) Centralized tracking, "*My Studies*" dashboard consolidates consents, statuses and histories; (b) Term change alerts, notifications when study terms change; (c) Outcomes feedback, links to publications, lay summaries and dashboards; and (d) Human support, accessible chat or email support during consent-critical junctures. Design recommendations encourage developing a "*My Studies*" dashboard with timelines and status filters, implementing term-change alerts, and providing accessible human support.

### 9.7.5 Theme 05: Usability and User Interface Experience (Researchers)

Researchers consistently emphasized that the platform is easy to use and intuitive. Ease of navigation was crucial for completing tasks efficiently. One respondent praised the interface but noted that certain elements did not behave as expected, such as "*conflicts with the expectations … not being able to click survey names*".

Illustrative Excerpts – Researchers described the interface as "*easy*" or "*very easy*" to navigate, highlighting the intuitive nature of the platform. They appreciated that the system allowed them to perform tasks quickly and with minimal friction. However, minor inconsistencies, such as non-clickable survey names, were perceived as jarring and should be addressed.

Subthemes and Design Implications – Subthemes included: (a) interaction consistency, list titles behave as links, buttons are styled and placed uniformly, and focus/hover states are predictable, creating a stable interaction grammar; (b) information scent and wayfinding, clear labels, breadcrumbs, and a global, type-ahead search to surface studies, participants, and forms quickly; (c) task-flow efficiency, batch actions,

sensible defaults, remembered filters/sorts, and keyboard paths to compress frequent workflows; and (d) error prevention and recovery, inline validation, undo, autosave, and consequence-aware confirmations to maintain speed without sacrificing safety. Design recommendations are to standardize click targets and control patterns, introduce global search and persistent breadcrumbs, add batch tooling and keyboard accelerators, and implement guardrails with reversible actions and draft autosave.

### 9.7.6 Theme 06: Centralized Study Management and Participant Tracking (Researchers)

Researchers value having a unified location for managing research studies and participants. They highlighted features such as enrolment management, re-enrolment automation and participant tracking, emphasizing that centralization reduces administrative overhead and cognitive burden.

Illustrative Excerpts – Respondents praised Consentio for providing a "*centralized location to keep track of all research studies*" and to "*get updates*". Participants also cited "*study management*" and "*dynamic consent management*" as the most useful features. One researcher suggested adding functionality to "*track an individual participant's status and see their participation as a timeline*" pointing to the demand for longitudinal monitoring.

Subthemes and Design Implications – Subthemes included: (a) longitudinal timelines, per-participant and per-study sequences of consent, messages, data pulls, and outcomes with event/actor filters and deep links to receipts; (b) enrolment and re-consent automation, policy-driven schedules keyed to protocol versions, expiries, and term changes; (c) audit and compliance views, one-click answers to who did what, when, and under which legal basis, rendered in human- and machine-readable formats; and (d) cross-study portfolio metrics, operational KPIs, with drill-through to underlying records. Design recommendations are to ship an auditable timeline view with export (PDF/CSV), a rules engine for re-consent and reminders, a "*Compliance Report*" generator (JSON/PDF), and a portfolio dashboard for prioritization.

### 9.7.7 Theme 07: Customization and Personalization (Researchers)

Several researchers expressed a desire to customize the interface and search results. Customization involves filtering options, starred or favourite studies, archiving, copying forms, importing standard questionnaires and adjusting visual settings such as dark mode and chart colours.

Illustrative Excerpts. Researchers requested "*filtering options when searching for studies to match specific interests*" the ability to "*star frequently accessed studies*", "*archive studies*", "*copy forms*" or import standard questionnaires. They also called for a "*dark mode*" and the ability to customize dashboard layout and chart colours to suit personal preferences.

Subthemes and Design Implications – Subthemes included: (a) interface filtering and favourites, saved searches, starred studies, quick filters, and lightweight archiving to preserve working contexts and accelerate retrieval; and (b) visual and layout options, dark mode, high-contrast and colour-blind-safe palettes, and role-aware page composition to improve comfort and inclusivity. Design recommendations are to enable named, shareable saved views with favourites, provide cloning of common configurations under version control where appropriate, and add an accessibility-checked theme switcher with layouts that foreground permitted actions for PIs, coordinators, and data managers.

### 9.7.8 Theme 08: Communication and Notification Preferences & Data Presentation (Researchers)

Researchers discussed ways to improve notifications, communication and data presentation. They sought timely and accessible communication mechanisms and better organization of charts and data displays.

Illustrative Excerpts. Suggestions included introducing a "*notification badge to indicate pending actions*", adding email reminders for re-consenting, presenting help messages in "*bullet points*", providing more information texts or context-sensitive help for specific fields, and using different colours in charts to enhance readability. Researchers also asked for improved chart organization and better data visualization layouts.

Subthemes and Design Implications – Subthemes included: (a) notification preferences, badges for unread and due-soon/overdue states, optional daily/weekly digests, and deep links to the precise action required; and (b) data organization, improved chart layout and legends, standardized axes and scales, annotations for consent/version events, CSV/PNG export, and context-sensitive help and microcopy to translate technical or regulatory commitments. Design recommendations include implementing a first-class notification centre with template-driven email reminders recorded as audit events, and standardizing the visual grammar and download options while embedding just-in-time helpers that render data intelligible at a glance.

## 9.8 Cross-Theme Tensions and Synthesis

Several tensions cut across the themes. Efficiency versus informedness emerged as a central dilemma: both participants and researchers appreciated expedited pathways (e.g., skip-ahead buttons and streamlined interfaces), yet they warned that speeding through consent flows risks superficial agreement. Designing gating mechanisms that require a full read before shortcuts are unlocked, and offering recaps, can mitigate this tension. Security versus comprehensibility reflects the need to translate cryptographic assurances into human-readable commitments; robust security features inspire trust only when their meaning is clear. Revocation versus irreversibility highlights the pragmatic limits of data control: participants accept that published or lawfully retained artifacts endure, but they expect explicit acknowledgement of these constraints and tools to act upon what can be controlled. Personalization versus standardization raises the question of how much freedom users should have to customize the interface without compromising consistency and regulatory compliance. The analysis suggests that enabling flexible dashboards and filtering, while maintaining core structures and safe defaults, may strike an appropriate balance (Brooks et al., 2017; de Andrade Cardieri & Zaina, 2018; Eslami Andargoli et al., 2017; Heinold et al., 2025; Hosseini Teshnizi et al., 2021; Ontañón M, 2020; Rahimi et al., 2014; Safdari et al., 2012).

*Table 21 - Subthemes and Representative Codes.*

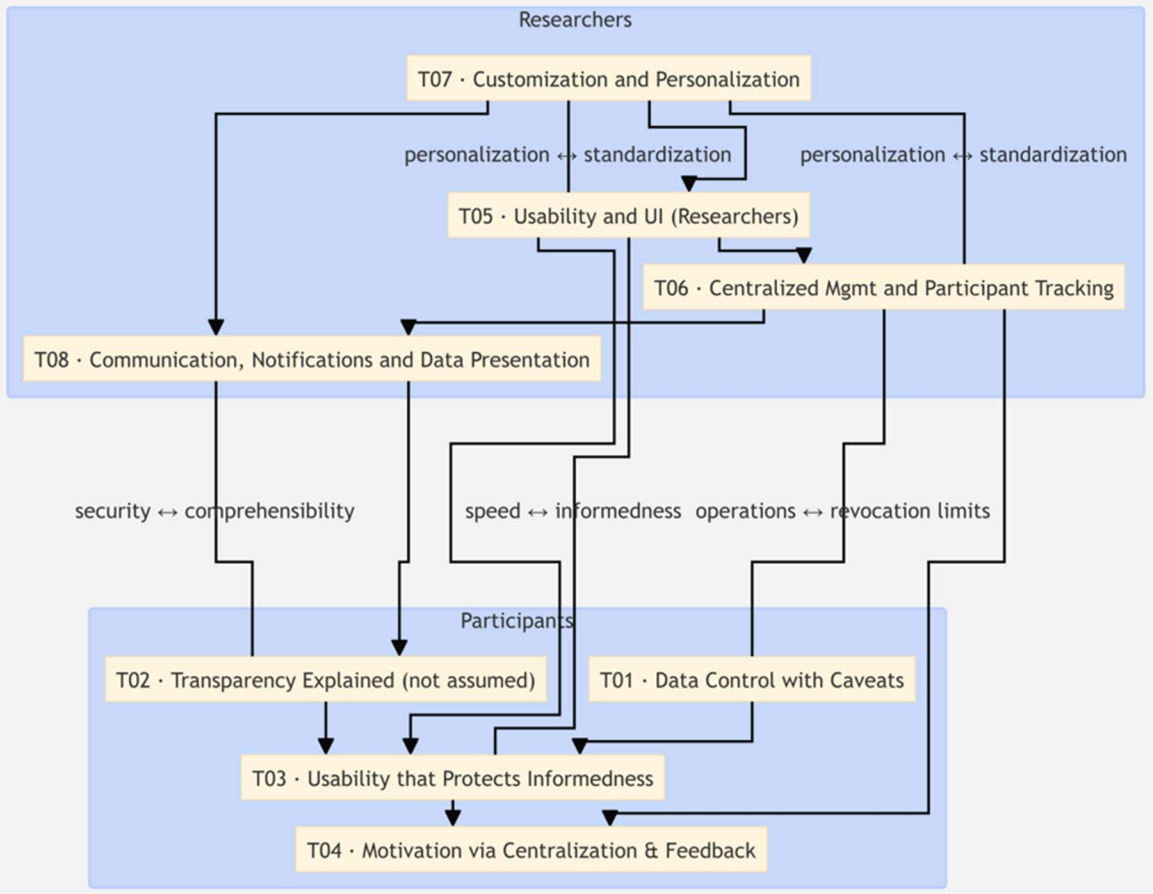
| THEME | SUBTHEME | REPRESENTATIVE CODES/PHRASES | SALIENCE |
|---|---|---|---|
| Data control with caveats | Revocation clarity vs. downstream copies | "*Revocation stops future access*"; "*legacy exports*"; "*published results*"; "*deletion windows*" | High |
| | Scope boundaries | "*API cut-off*"; "*visibility change*"; "*exceptions for lawful retention*"; "*provenance marks*" | Medium |
| | Actionability locus | "*Enroll/Pause/Withdraw*"; "status *badges*"; "*proof-of-action receipts*" | Medium |
| Transparency explained | Auditability reassures | *"Timestamped consent log"; "actor/time trace"; "verifiable receipts"* | High |
| | Plain-language security | *"Ledger vs. blockchain jargon"; "tamper-evidence"; "role-based access"* | Medium |
| Usability Protects Informedness | Progressive disclosure | *"Accordion summaries"; "expand details"; "cognitive load balance"* | High |
| | Skip-ahead tension | *"Convenience vs. comprehension"; "gating acknowledgements"* | Medium |
| Motivation Via Centralisation and Feedback | Centralized tracking & outcomes | *"My Studies hub"; "term change alerts"; "lay summaries"; "chat support"* | High |
| Customisation and Personalisation | Interface filtering & favourites | *"Filter studies"; "star frequently accessed"; "archive studies"; "copy forms"* | Medium |
| | Visual & layout options | *"Dark mode"; "customize dashboard"; "different colours in charts"* | Medium |
| Communication & Data Presentation | Notification preferences | *"Notification badge"; "email reminders"; "bullet-point help"* | Medium |
| | Data organization | *"Better organization of charts"; "context-sensitive help"; "data presentation improvements"* | Medium |

### 9.8.1 Comparison of Participant and Researcher Perspectives

Although participants and researchers approached Consentio from different roles, their perceptions converged on several points. Ease of use was recognized as a major strength by both groups, yet minor interface inconsistencies were noted. Centralization emerged as a valued feature for managing studies and data; participants saw it as a way to view all their research engagements and outcomes, while researchers highlighted administrative efficiency. Transparency was a shared concern: both groups wanted explanations that made security mechanisms intelligible. Personalization and communication were emphasized primarily by researchers, reflecting their need to tailor workflows and receive timely alerts. Participants placed greater emphasis on data control and motivation, underscoring their role as data subjects and their desire for feedback (Amoako-Gyampah, 2004; Funnell et al., 2022; Gonzalez et al., 2022; McGinn et al., 2011; Tong et al., 2018).

Figure 16 depicts a thematic map illustrating the relationships among themes. Data control and transparency form foundational layers that support usability and motivation; customization and communication modulate how users interact with the core layers. Tensions (e.g., efficiency vs. informedness) are represented by crossed arrows connecting the relevant themes.

*Figure 16 - Relationship between themes.*




## 9.9 Design Implications and Recommendations Summary

Building on the themes and cross-theme tensions, the following recommendations were extracted for future development of Consentio:

Enhance Revocation Interfaces – Implement a Revocation Outcomes panel that clearly describes what happens to data upon withdrawal, including deletion windows and exceptions for published analyses.

Provide status badges indicating enrolment, pause and withdrawal states and generate verifiable receipts for user actions.

Surface Export Controls During Consent – At the consent stage, show whether data can be exported, under what conditions and who will have access. Encourage study owners to declare export policies and commit to the deletion of external copies within specified time frames.

Translate Security Mechanisms – Develop a concise "*Why your data is safe here*" explainer with diagrams showing how the ledger protects data. Complement this with an access table listing actors, data items, legal bases, and durations for each study.

Balance Speed and Informedness – Allow skip-ahead functionality only after a complete first viewing, and gate enrolment behind toggles acknowledging key points. Provide just-in-time definitions and a final recap summarizing what the user has agreed to.

Build a Comprehensive Dashboard – Create a "*My Studies hub"* with timelines, status filters and term-change alerts for participants, and develop similar dashboards for researchers to track participant statuses and study metrics. Include links to publications and lay summaries to sustain motivation.

Enable Personalization – Offer filtering options, favourites, archiving and form-copying features. Allow users to customize dashboard layout, enable dark mode and choose colour schemes for charts.

Improve Communication and Data Presentation – Introduce notification badges and email reminders; present help information in concise bullet points; provide context-sensitive help; and refine chart organization with adjustable cooler palettes and clear legends.

## 9.10 Discussion

This section presents the synthesis of the research questions proposed in this section and their answers, extrapolated from the RTA results.

### 9.10.1 How Users Understand and Exercise Control Over Their Data

Across participant accounts, control was understood as the ability to take discrete, auditable actions, enroll, pause, withdraw, and to see proof that those actions had effect. Participants consistently located control within a visible "*locus of action*" in the interface, and they valued status badges and receipts that confirmed outcomes (Theme 01; Table 21: actionability locus). However, this sense of control was bound by a pragmatic awareness that once data have been exported or aggregated elsewhere, recall is limited. Participants distinguished between halting future access through API cut-offs and the irreversibility of prior dissemination, asking for plain statements about what withdrawal can and cannot accomplish (Table 21: revocation clarity vs. downstream copies; scope boundaries). In short, control was experienced as timely decisional authority inside the platform, tempered by the realities of downstream data flows.

Exercising control, therefore, depended as much on intelligible boundaries as on technical capability. Participants reported that confidence increased when the interface coupled actions with verifiable artifacts, time-stamped receipts, clear state changes, and audit-log pointers, and when revocation was framed with conditions, deletion windows, and lawful-retention exceptions. Researchers converged on this view, proposing a "*Revocation Outcomes*" panel that ties each action to its technical and legal consequences and surfaces export controls at the time of consent. The emergent interpretation is that effective control in dynamic consent is relational: it is enacted through UI affordances and proofs but secured through truthful scoping of obligations beyond the platform.

### 9.10.2 What Signals and Explanations Foster Transparency and Trust

Trust was not fully delivered by the ledger; it emerged when cryptographic guarantees were translated into human-readable commitments. Participants and researchers pointed to immutable, time-stamped consent logs and actor traces as reassuring yet repeatedly emphasized that auditability becomes meaningful only when users understand what is recorded, why it matters, and who can see it (Theme 02; Table 21: auditability reassures; plain-language security). Requests for an access table, articulating actors, data items,

legal bases, and durations per study, illustrate that "*transparency that is explained, not assumed*" hinges on situated explanations that map technical mechanisms to everyday consequences.

The credibility of those signals was further strengthened by communication design. Brief, scannable explainers ("*Why your data is safe here*"), in-context microcopy, and diagrams linking ledger entries to data-handling protections made the private-ledger architecture legible. On the researcher side, notification and presentation practices (Theme 08; Table 21: data organization; notification preferences) also served as trust signals: consistent legends, stable scales, and annotated events in dashboards conveyed a disciplined stewardship of information. In summary, trust cohered where two layers met, tamper-evident records and comprehensible narratives that specify rights, duties, and limits.

## 9.11 Which Aspects of Usability Support or Threaten Informed Consent

Participants experienced Consentio as easy to navigate, but remained alert to the risk that speed can eclipse understanding. Progressive disclosure and brief recap screens were welcomed because they manage cognitive load while preserving the integrity of consent (Theme 03; Table 21: progressive disclosure; confirmation recap). By contrast, unconstrained skip-ahead behaviour, especially on the first visit, was read as a threat to informedness. The procedural resolution favoured in the data is straightforward: unlock shortcuts only after a complete first pass viewing and gate enrolment behind concise acknowledgements of key points (Table 21: skip-ahead tension).

Researchers reinforced the same balance from an operational angle. They asked for consistent interaction and predictable controls to reduce friction without creating paths that bypass comprehension (Theme 05). Batch tooling and keyboard accelerators are appropriate for researcher workflows; participant-facing flows should prominently feature comprehension safeguards. The synthesis is a design stance that treats usability and informedness as co-requirements: efficiency is encouraged within role-appropriate contexts, while enrolment actions remain coupled to minimal, verifiable understanding.

### 9.11.1 Which Factors Motivate or Discourage Continued Participation in Public Health Research

Motivation was sustained when people could see and manage their research lives in one place and when the outcomes of their contributions were made visible. A centralized "*My Studies*" hub that consolidates consents, statuses, histories, and term-change alerts supported a durable sense of agency over time, reducing the effort of remembering where and how one had consented (Theme 04; Table 21: centralized tracking; term-change alerts). Participants contrasted this clarity with prior paper-based experiences, noting that simple cues, status badges, timelines, and receipts made participation feel tractable rather than diffuse. Closing the loop with links to publications and laying summaries further validated the effort by turning the contribution into something observable and consequential (Table 21: outcomes feedback).

Discouragement, by contrast, arose from ambiguity and silence. Unclear revocation boundaries undermined confidence that choices would travel with their data; delayed responses to queries or the absence of timely notifications about protocol changes gave the sense that studies "*went quiet*." Participants framed these gaps as motivational, not merely informational: uncertainty about what happens next weakens the willingness to remain enrolled. Both cohorts therefore endorsed human-in-the-loop support, auditable chat, clear escalation to a PI or ethics officer, and notification practices that translate protocol dynamics into concrete prompts to act (Theme 08; Table 21: notification preferences).

Taken together, the evidence suggests that continued participation depends on two intertwined affordances: longitudinal visibility over one's trajectories and credible, timely communication that demonstrates the study is active, responsive, and worthy of attention. The first is implemented through a well-instrumented hub, timelines, outcome links, and term-change alerts, so that participation is legible immediately. The second is delivered through a first-class notification centre and templated, auditable messages that deep-link to the exact action required, turning background change into intelligible next steps. When combined, these practices couple motivation to governance: participants can both see their past and know what to do now, while researchers meet compliance needs without sacrificing relational trust.

## 9.12 Conclusion

Taken together, the findings suggest that dynamic consent, to function as more than an interface veneer, must integrate three mutually reinforcing capacities: revocation realism, operational transparency, and informed speed (Dankar et al., 2020; Mascalzoni et al., 2022; Prictor et al., 2020; Scott et al., 2018). Revocation realism names the alignment problem most salient to participants; people are comfortable exercising control when the system states plainly what withdrawal will and will not do, especially regarding prior exports and lawful-retention artifacts. Major ethics and privacy frameworks anticipate this boundary, for example, the Tri-Council Policy Statement in Canada (Canadian Institutes of Health Research, 2022) frames consent as "free, informed, and ongoing," and recognizes that withdrawal rights may be limited once data are de-identified or already used in analyses, while still requiring clear communication about those limits; similarly, the GDPR (European Parliament and of the Council of 27 April 2016, 2016; Tovino, 2017) recognizes a right to erasure that is constrained for scientific research when appropriate safeguards are in place under Article 89 (Canadian Institutes of Health Research, 2026b; European Parliament and Council of the European Union, 2016e; Natural Sciences and Engineering Research Council of Canada, 2026; Social Sciences and Humanities Research Council of Canada, 2026).

The recommended Revocation Outcomes panel and access tables convert a diffuse legal-technical space into a navigable set of expectations, reducing the gap between decisional authority and practical effect. These reframing moves matter because consent is not merely a prior authorization, it is an ongoing governance relation whose legitimacy depends on the credibility of future-oriented claims; by surfacing scope boundaries and deletion windows at the moment of decision, the platform invites informed agency rather than tacit acquiescence to unknown constraints (Canadian Institutes of Health Research, 2026b; Natural Sciences and Engineering Research Council of Canada, 2026; Social Sciences and Humanities Research Council of Canada, 2026).

Operational transparency addresses a distinct but related deficit, without translation, the very mechanisms intended to guarantee integrity can erode trust by reading as "background magic." The ledger

creates an immutable trace, but users, participants and researchers, seek intelligibility, what constitutes a consent event, which actors are implicated, how timestamps relate to actions, and how those records travel into audit and compliance contexts. Regulatory texts directly support this translation layer. GDPR Article 12 (European Parliament and Council of the European Union, 2016a) requires information that is concise, transparent, intelligible, and easily accessible, with plain language and, where appropriate, visualization, while Articles 13 and 14 (European Parliament and Council of the European Union, 2016b, 2016c),require communicating recipients, purposes, and retention periods, which maps neatly to a per-study "access table" that lists actors, data items, legal bases, and durations(European Parliament and of the Council of 27 April 2016, 2016).

In regulated research contexts, audit trails are not optional; 21 CFR Part 11(Health Canada, 2021; U.S. Food and Drug Administration, 2026b), requires secure, computer-generated, time-stamped records of user actions, with changes that do not obscure prior entries and that are retained for inspection, and FDA's e-consent guidance recommends documenting the electronic consent process and ensuring traceability of interactions such as signatures and acknowledgements (U.S. Food and Drug Administration, 2026a, 2026c).

When combined with participant-readable explainers and annotated timelines, these requirements convert cryptographic immutability into organizational accountability. Researchers' desire for one-click compliance reports and portfolio KPIs extends the same logic, transparency is not a single log, it is a set of situated views, historical, managerial, and evidentiary, that enable different roles to answer for their stewardship. In this sense, the section's theme map is also a governance map, participant-side transparency practices anchor researcher-side management practices, and both sides depend on clear, shared representations of events and obligations (U.S. Food and Drug Administration, 2026e).

Informed speed articulates the central tension running through the corpus, stakeholders want to move quickly, but not at the expense of understanding. Contemporary guidance reinforces this balance. OHRP and FDA require that information be conveyed "in language understandable" to the subject, and

recent federal draft guidance emphasizes designing consent to facilitate understanding by foregrounding key information, which supports recap screens, micro-acknowledgements of critical points, and layered content that defers detail until it is relevant (Office for Human Research Protections, 2026; U.S. Food and Drug Administration, 2026f).

Likewise, FDA's e-consent guidance encourages electronic strategies that ensure participants actually access and review the consent content before signing, a direct rationale for gating enrolment on a first complete pass through the materials (U.S. Food and Drug Administration, 2026g).

Human-factors evidence aligns, progressive disclosure reduces cognitive load and error likelihood by revealing complexity in stages, which supports your findings that accordion summaries and just-in-time definitions aid comprehension without blocking flow, and that shortcuts should be conditional, not universal (Jakob Nielsen, 2006).

For researcher workflows, the same literature stresses consistency and standards, predictable controls reduce errors and speed expert tasks, which validates standardizing clickable regions, button grammar, and navigation scaffolds across Consentio modules (Jakob Nielsen, 2024). What emerges is a layered usability strategy, accelerate where repetition dominates and comprehension is already secured, slow down where the moral and legal weight of the decision demands it.

The motivational economy of participation further demonstrates why these capacities must be integrated rather than sequential. Centralization increases the salience of control and reduces the administrative load of participation, but it also creates an obligation to curate feedback. Empirical and normative guidance points the same way, dynamic consent is conceived as a personalized digital interface that supports ongoing choices, recontact, and two-way communication, thereby sustaining engagement over time, and it explicitly envisions keeping a record of transactions in one place that participants can revisit (Kaye et al., 2015b).

Return of results, whether aggregate lay summaries or individual findings where appropriate, is increasingly seen as good practice that can strengthen trust, improve satisfaction, and support retention; multi-stakeholder guidance from the MRCT Center provides practical frameworks and toolkits for returning results in plain language via portals or digests, which maps closely to your proposals for outcomes links and notifications in the hub (MRCT Center, 2022, 2024).

When notifications are auditable and context-linked, they bridge compliance interests with participants' dignity interests; they also fulfill transparency duties under GDPR and similar regimes that call for clear, accessible communication about processing and changes over time (European Parliament and of the Council of 27 April 2016, 2016).

Methodologically, the critical realist orientation clarifies why themes are presented as analytically constructed rather than as discovered essences. The recurrent patterns here, revocation boundaries, explained transparency, informed speed, centralized feedback, index real pressures in consent practice without claiming ontological finality. They are credible because they are reflexively derived, triangulated across roles, and tied to concrete artifacts such as receipts, timelines, and dashboards. This stance also disciplines claims about generalizability; the sample is small and digitally literate, but the design tensions it illuminates are likely portable across settings that combine digital consent capture with distributed data handling. Future work can test these constructs quantitatively, for example, by measuring comprehension under gated versus ungated flows, or trust under access-table versus no-table conditions, and extend the qualitative lens to populations with different literacy profiles. Existing federal guidance already encourages comprehension-first consent and the use of layered key information; these provide immediate experimental levers for evaluation designs that compare gated flows with baseline patterns (Office for Human Research Protections, 2026; U.S. Food and Drug Administration, 2026f, 2026e, 2026a).

Finally, the implications for implementation are practical and immediate. Prioritize building the Revocation Outcomes panel and per-study access tables, instrument the participant "My Studies" hub with timelines and outcome links, adopt a notification centre with deep-linked, auditable prompts, and

standardize interaction grammar across components. Collectively, these moves do not merely add features; they instantiate a socio-technical contract in which consent is actionable, transparency is legible, and speed is conditional on understanding. Such a contract is the precondition for scaling dynamic consent in public-health research without diluting its ethical core, and it is defendable under the leading ethics and privacy frameworks that emphasize ongoing consent, transparency, and accountable records of action (Canadian Institutes of Health Research, 2026b; European Parliament and of the Council of 27 April 2016, 2016; Natural Sciences and Engineering Research Council of Canada, 2026; Office for Human Research Protections, 2026; Social Sciences and Humanities Research Council of Canada, 2026; U.S. Food and Drug Administration, 2026f).

# 10 Summary of Design Recommendations for a Governance Guided, Blockchain-based, Tailored for Public Health Research That Leverages Personal Health Information Dynamic Informed Consent Management Platform

## 10.1 Introduction

The preceding thematic synthesis bridges the empirical findings with the theoretical and technical foundations laid in Sections 6, 7, 8, and 9. Across the interviews and surveys, participants repeatedly emphasized three intertwined capacities: (i) revocation realism (clear boundaries on withdrawal), (ii) operational transparency (plain-language explanations and auditable trails), and (ii) informed speed (efficiency conditioned on comprehension); Which mirror and refine the critique of traditional informed consent set out in Section 1, and the data-governance framework developed in Section 6. They also highlighted the motivational role of a unified hub that consolidates studies, shows outcomes, and provides auditable notifications. These insights guide a re-examination of the historical evolution of consent, the proposed governance framework, and the Consentio platform described in Section 7.

## 10.2 Aligning User Experiences with the Broader Research Context

Sections 1 through 5 traced the transformation of consent from paternalistic medical oaths to codified principles such as the Nuremberg Code and the Declaration of Helsinki. Early models rarely contemplated participant withdrawal, data reuse, or ongoing engagement. Contemporary regulations recognize these gaps. For example, the Tri Council Policy Statement in Canada notes that where research terms do not allow for the withdrawal of data or biological materials, the identity of participants must be protected. Similarly, the GDPR requires information to be communicated “in a concise, transparent, intelligible, and easily accessible form”. These provisions mark a shift toward acknowledging participant autonomy while recognizing practical limits on revocation (European Parliament and of the Council of 27 April 2016, 2016;

Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2022) – Chapter 3: The Consent Process, 2022).

Section 6 builds on this historical context by proposing a governance framework for public-health research that balances data utility with respect for individual autonomy. It identifies four shortcomings of traditional informed consent: (i) consent fatigue and information overload; (ii) lack of participant empowerment; (iii) inadequate data governance mechanisms; and (iv) absence of scalable, technology-enabled processes. Our findings resonate strongly with these critiques. Participants lauded Consentio's capacity to centralize consent management and record all actions, thereby overcoming the fragmentation of paper- or email-based consent. Yet many interviewees felt overwhelmed by long consent documents and alerts; 86 % explicitly raised concerns about information overload. They also sought assurances that withdrawal would stop future access while recognizing that some data cannot be erased once used in publications. Such requests align with the notion of revocation realism, making explicit what withdrawal can and cannot accomplish.

Table 22 maps the challenges identified in Section 6 to updated themes from the usability study. The "*Data Control With Caveats*" theme now encompasses both revocation realism (clarity on downstream copies) and actionable loci (enroll, pause, withdraw). "*Transparency That Is Explained*" integrates operational transparency, emphasizing plain-language security and auditability. "*Usability That Protects Informedness*" maps onto informed speed; progressive disclosure and recap screens are considered necessary to mitigate consent fatigue. "*Motivation Sustained by Centralization and Feedback*" extends the original "*user empowerment*" challenge by highlighting the motivational role of consolidated dashboards and outcome feedback. The table summarizes the alignment between Section 6's problem statements and the participants' lived experiences.

*Table 22 - Mapping of Section 6's challenges into themes.*

| Challenge from Section 6 | Description | Theme | Evidence from participants |
|---|---|---|---|
| Consent Fatigue & Information Overload | Participants disengage when confronted with long, dense materials and frequent alerts; they want summaries and gated flows. | Usability That Protects Informedness | 86% voiced frustration about information overload and asked for summarized consent, progressive disclosure, and recap screens. |
| Lack Of Participant Empowerment | Traditional consent limits control over sharing and withdrawal; users want actionable controls and receipts. | Data Control with Caveats | Interviewees valued being able to enroll, pause, withdraw, view status, and receive proof-of-action receipts in real time; they also asked for clear boundaries on what withdrawal can/cannot stop. |
| Inadequate Data Governance | Governance gaps undermine trust; users want auditable trails and role-based access that they can understand. | Transparency That Is Explained, Not Assumed | Participants cited immutable audit trails and role-segregated access as trust-building; 80% were "*very likely*" and 20% "*likely*" to recommend, often tying trust to transparency. |
| Need For Scalable, Technology-Enabled Consent | PHI/wearables demand a centralized, responsive hub that scales with clear navigation and status visibility. | Motivation Sustained by Centralization and Feedback | Users praised centralized dashboards for tracking consents and outcomes, but urged better navigation, summaries, and performance tuning to support broader adoption. |

Section 6 also introduced dynamic consent as a way of addressing these challenges by enabling continuous two-way communication and supporting autonomy. Dynamic consent has been described as a personalized interface that enhances engagement and allows participants to "*keep track of their data*" and the donations they have made (Cocanour, 2017; Dankar et al., 2020; European Parliament and Council of the European Union, 2016c; Health Canada, 2021; Kaye et al., 2014; Mascalzoni et al., 2022; U.S. Food and Drug Administration, 2026e, 2026a, 2026c, 2026b). Participants in our study affirmed these benefits, highlighting the importance of checking consent status, adjusting preferences, and viewing historical actions, but cautioned that the underlying technologies (e.g., blockchain) must be explained in simple language. They called for accessible diagrams and tables summarizing who can access what and under

which legal basis, underscoring that technology alone cannot overcome historical mistrust without user-centred communication.

### 10.2.1 Comparing User Feedback with Platform Design

Section 7 describes Consentio's modular architecture and its operationalization of the governance framework through Hyperledger Fabric, NodeJS microservices, and an Angular front-end (Google Inc., 2026; Hyperledger Foundation, 2026b, 2026c; HyperledgerDocs, 2018). Four aims guide the design: (1) enforce the governance framework; (2) implement a secure, segregated architecture; (3) adopt technologies supporting data sovereignty, auditability, transparency, and revocability; and (4) build a minimum-viable platform. Table 22 compares these design features with the updated themes and user perceptions.

*Table 23 - Cross-analysis of Section 7 design features and user feedback.*

| Design Feature / Governance Requirement | Implementation Details | User Perception & Updated Theme | Alignment / Discrepancy |
|---|---|---|---|
| Immutable Audit Trail & Append-Only Ledger | Fabric chaincode records consent actions; endorsement policies include IRB peers before commit. | Auditability reassures; users tie trust to timestamped logs and receipts → Transparency That Is Explained, Not Assumed. | Strong alignment on integrity; some requested clearer "how logs are used" explainers. |
| Role-Segregated Private Channels | Channels segregate investigators, custodians, and IRBs; only need-to-know parties see records. | Users liked role-segregated views but want clearer "who has access/was contacted" visualizations → Transparency That Is Explained, Not Assumed and Data Control with Caveats. | Partial: technical segregation exists; the interface should expose actor roles and statuses more explicitly. |
| Real-Time Revocation & Event Listeners | World-state updates plus events notify UI in < 500 ms. | Valued ability to revoke; want plain-language outcomes for downstream copies/exports → Data Control with Caveats. | Partial: capability present; communication of post-revocation effects needs improvement. |
| Responsive & Accessible Interface | Angular + Bootstrap; WCAG 2.1 AA. | Generally easy to use, but dense information and occasional lags hinder experience; users asked for progressive disclosure, tooltips, and short tutorials → Usability That Protects Informedness. | Mixed: standards met, but progressive disclosure, summaries, and pacing aids are needed to reduce cognitive load; occasional performance tuning noted. |
| Off-Chain Storage With Hashed References | Documents stored off-chain (SQL/Postgres) with on-chain hashes. | Integrity appreciated; a subset raised sustainability/energy questions—address via transparent messaging → Transparency That Is Explained, Not Assumed. | Aligned on integrity; add sustainability explainers to improve acceptance. |
| Api Orchestration & Modular Microservices | NodeJS microservices; rate-limiting; token auth. | Backend not a user focus; occasional latency observed—monitor as scale grows → Usability That Protects Informedness (pacing). | Alignment unassessed by users; watch performance and tighten where needed. |

This analysis shows that many technical features achieve their intended purpose, ensuring integrity, segregation and revocability, but user feedback underscores the importance of explanatory resources and interface refinements. For instance, real-time revocation is built into the code, yet participants remain uncertain about data deletion; similarly, a WCAG-compliant interface can still overwhelm users without progressive disclosure. Aligning design with the updated themes, therefore, involves not only engineering compliance but also redesigning the user experience around key capacities identified in the qualitative study.

### 10.2.2 Integrating Digital Literacy and Self-efficacy into the Design

Section 6 notes that the spread of PHI from wearables and sensors requires inclusive consent frameworks that account for varied digital abilities. Research shows that digital ability declines with age and is influenced by income and education (Hargittai et al., 2019; Hargittai & Dobransky, 2017; Neves et al., 2013). In our evaluation, participants were mostly young, highly educated and technologically proficient; they rated their operational and information skills highly (ISS ≈ 4.14) and reported relatively high self-efficacy (CUSE ≈ 2.97 on a 1–6 scale). However, the distribution of CUSE responses included both strong agreement and strong disagreement, indicating a polarity in confidence levels. Designing for broader audiences, including older adults and those with lower digital literacy, thus demands additional support mechanisms.

Revocation realism and operational transparency must be communicated in accessible ways; complex legal or blockchain terms should be avoided. Progressive disclosure, layered information, and guided tutorials can mitigate consent fatigue and support comprehension. The modular architecture described in Section 7 enables such adaptations. For instance, dynamic forms can be simplified for users with low literacy, while advanced dashboards remain available for researchers. Expanding interface modes (e.g., “basic” and “advanced” views) can accommodate this diversity.

### 10.2.3 Theoretical Intersections: Consent Models, Autonomy and Technology Adoption

Dynamic consent merges ethical principles with technological innovation. Scholars describe it as a personalized interface that enables participants to "*keep track of their data*" and adjust consent over time (Canadian Institutes of Health Research, 2026b; European Parliament and Council of the European Union, 2016c; Kaye et al., 2015b; U.S. Food and Drug Administration, 2026g, 2026c, 2026b). Blockchain technologies support this autonomy by providing tamper-evident, time-stamped audit trails; audit trails are required by regulations such as 21 CFR Part 11, which emphasizes computer-generated, time-stamped records to capture creation and modification actions (U.S. Food and Drug Administration, 2026f). However, as participants noted, auditability does not equate to trust unless accompanied by plain-language explanations. GDPR Article 12 (European Parliament and Council of the European Union, 2016a) requires that information be communicated in clear and plain language, underscoring the role of communication design.

The themes also intersect with social cognitive theory. Engagement with digital tools depends not only on system design but also on users' belief in their ability to use those tools effectively. Our observation that higher CUSE scores correlated with higher Net Promoter Scores suggests that self-efficacy influences adoption. Thus, dynamic consent platforms must support skill development through intuitive interfaces, help texts, and responsive support, alongside technical safeguards. Importantly, progressive disclosure is more than a usability feature; it has been shown to reduce cognitive load and errors by transferring advanced or rarely used features to secondary screens (Ontañón M, 2020). Combining these theoretical insights with our updated themes underscores that autonomy is realized through a socio-technical contract: participants exercise choice within boundaries, while the system honours transparency and provides responsive support (Bandura, 2001; Saksono & Parker, 2024; Schunk & DiBenedetto, 2020; Steelman et al., 2016; Tao et al., 2020).

### 10.2.4 Future Considerations and Integration with Broader Thesis Findings

Sections 1 through 6 set the conceptual and ethical context for consent, whereas Section 7 operationalizes those principles through the Consentio platform. The mixed-methods evaluation demonstrates that the platform largely achieves its goals: it enhances trust, empowers participants, and meets core governance requirements. However, the updated themes highlight areas for refinement. Addressing consent fatigue through progressive disclosure, clarifying data retention limits, and enhancing visibility of study and participant statuses will be essential for broad adoption. Table 25 summarizes how insights from Sections 1-5 (historical consent), 6 (governance framework), and 7 (system architecture) converge into the updated themes.

*Table 24 - Cross-section synthesis of thesis findings.*

| Section / Dimension | Historical/Theoretical Insight | Updated theme | Design or policy implication |
|---|---|---|---|
| Sections 1-5 – Informed Consent History | Early consent models lacked explicit withdrawal procedures; later frameworks recognize that some data cannot be withdrawn once used. | Revocation realism | Clarify at consent time what withdrawal means; provide receipts and outcome panels. |
| | Paternalistic communication has given way to requirements for clear, plain-language information. | Operational transparency | Develop human-readable security explainers and access tables; avoid jargon. |
| Section 6 – Data Governance Framework | Modern public-health research requires robust data governance; consent fatigue, lack of empowerment and inadequate governance are key challenges. | Informed speed; motivation | Implement progressive disclosure; consolidate consents and notifications in a single hub; support dashboards. |
| | Inclusive frameworks must account for varied digital literacies. | Digital literacy | Provide guided tutorials, simplified summaries, and layered information; develop basic/advanced interface modes. |
| Section 7 – Platform Development | Hyperledger Fabric and modular microservices implement integrity, segregation, and revocability, but user understanding is critical. | All themes | Align technical features with user-centred explanations; adjust interface to expose status and actions; monitor performance. |

Future iterations should leverage the modular architecture to introduce role-aware dashboards, context-sensitive help, and sustainability messaging (to address concerns about blockchain's environmental impact) (Wendl et al., 2023). Exploring interoperability with self-sovereign identity standards and other research platforms could extend the platform's reach and align it with broader ecosystem goals. Continued evaluation should include task-based studies testing comprehension under gated versus ungated flows,

experiments assessing trust with and without access to tables, and field deployments with diverse user populations. Such work will ensure that dynamic consent platforms like Consentio fulfil their promise of transforming research participation in the digital age.

# 11 Limitations

This section prioritized thick description, triangulation across roles, and a documented audit trail to enhance credibility and dependability. Credibility was pursued by preserving rich, role-specific excerpts, by actively seeking negative cases that challenged early interpretations, and by maintaining traceability from codes to themes through a version-controlled codebook and decision log. Reflexivity was treated as a resource, not a threat; positionality memos recorded how disciplinary background and prior exposure to consent technologies could shape meaning-making during coding and theme development, consistent with reflexive thematic analysis practice (Braun et al., 2022; Braun & Clarke, 2006, 2019, 2021; Campbell et al., 2021). Dependability was supported through dated memos, explicit inclusion and exclusion criteria for each theme, and reproducible links from exemplary extracts to the final narrative. Confirmability was addressed by aligning interpretive claims with inspectable artifacts, such as time-stamped audit receipts, annotated timelines, and theme maps that show how interpretations followed from data excerpts and cross-role comparisons.

In addition to these methodological constraints, the participant pool was limited to a specific geography (Toronto, Canada) and comprised individuals with relatively high levels of education and digital proficiency. Interviews were conducted in English, and participants were predominantly young adults, which means the themes that emerged may not fully capture the experiences of older adults, those with low digital literacy, or research contributors from different linguistic or cultural contexts. Self-selection into the study may also have introduced bias, as people willing to volunteer for research about consent management may already hold positive attitudes toward digital platforms. These factors suggest caution when generalizing the findings. Future work should recruit larger, more diverse samples across age groups, education levels, languages, and jurisdictions, and should incorporate longitudinal observations to validate and refine the design implications outlined in this section.

This matters because a platform that works well for highly educated and digitally confident users may still impose burdens on older adults, people with lower digital literacy, people with limited English

proficiency, people with disabilities, or communities with different relationships to health research. Future work should therefore include purposive recruitment across education, age, language, disability, rural/urban access, and digital-access groups, and should test whether interface supports such as plain-language summaries, multilingual content, assisted consent workflows, and alternative notification channels reduce those burdens.

Other limitations that should be acknowledged: The small, digitally literate sample narrows the breadth and reduces statistical generalizability; findings are theory-building and design-oriented rather than representative. The study relied on self-reported perceptions; observed behaviour under real workload or time pressure may differ. Interviews were cross-sectional; they captured situated sense-making at one point in time rather than longitudinal change. Researcher reflexivity implies that themes are interpretive constructions rather than discovered essences; this aligns with the epistemology of reflexive thematic analysis, but it also means alternative, equally defensible mappings are possible (Braun & Clarke, 2019, 2024b). Platform novelty and social desirability effects may have inflated positive judgments of transparency or usability. Jurisdictional variability in ethics and privacy regimes may constrain transferability; while the analysis references widely adopted requirements such as ongoing consent, transparent communication, and auditable records, concrete obligations differ by regulator and institution. Finally, comprehension was inferred from interview accounts and design preferences; future work should include task-based studies with comprehension checks, gated versus ungated flows, and re-consent scenarios that introduce real changes in terms, so that claims about informedness can be tested directly. Despite these limitations, the combination of thick description, reflexive transparency, and an auditable trail provides a defensible basis for the design implications reported here (Campbell et al., 2021).

# 12 Overarching Conclusions

The reflexive thematic synthesis demonstrates that Consentio delivers on core promises of ease of use, centralized study management, and dynamic consent, while also revealing the conditions under which these promises are credible in practice. End-users valued a unified hub where they could enroll, pause, and withdraw; they especially valued visible proofs of action such as status badges, receipts, and timelines. Participants' sense of control, however, depended on clear boundaries around withdrawal and honest acknowledgement of downstream limitations. Researchers echoed this need for clarity and proposed concrete mechanisms, for example, a Revocation Outcomes panel and per-study access tables that specify actors, data items, legal bases, and retention windows. Trust did not arise from the presence of a private ledger alone; it arose when audit trails and cryptographic guarantees were translated into plain-language explanations and situated views that make the system's protections legible.

Usability emerged as a joint requirement with informedness. Progressive disclosure, recap screens, and just-in-time definitions helped participants manage cognitive load, while procedural safeguards such as unlocking shortcuts only after a complete first-pass viewing protected the integrity of consent. On the researcher's side, interaction consistency, predictable controls, and role-appropriate accelerators reduced friction without creating pathways that bypass understanding. Motivation to participate was amplified by centralization and feedback. A well-instrumented "My Studies" hub, with timelines, term-change alerts, and links to publications or lay summaries, turned participation into a legible, ongoing relationship rather than a one-time transaction. Notification practices that are auditable and deep-linked connected day-to-day action to compliance needs and dignity interests, for example by transforming protocol changes into clear prompts that explain what is changing and what the participant can do.

The synthesis points to a practical implementation agenda. First, build the Revocation Outcomes panel and per-study access tables, and surface export controls and retention conditions at the moment of consent. Second, instrument the participant hub with timelines and outcome links, and provide a notification centre that issues due-soon and overdue prompts and lands users on the precise action required. Third,

standardize interaction grammar across components, for example clickable regions, labels, and control placement, and adopt recap and acknowledgement steps that make key information explicit before enrolment. Fourth, provide researcher-facing views that are historical, managerial, and evidentiary, for example one-click compliance reports, portfolio metrics with drill-through, and annotated event timelines. These moves do not merely add features; they instantiate a socio-technical contract in which consent is actionable, transparency is legible, and speed is conditional on understanding.

Methodologically, the section shows how a critical-realist stance and reflexive thematic analysis can surface design tensions that matter for both ethics and operations. Themes were treated as interpretive constructs grounded in recurrent patterns, not as essences; credibility was sought through openness about the analyst's position, through triangulation across roles, and through an audit trail that allows others to interrogate decisions and mappings from code to theme to recommendation (Braun et al., 2022; Braun & Clarke, 2019, 2024b; Campbell et al., 2021). Looking ahead, the next phase should pair iterative builds with mixed-methods evaluation. Task-based experiments can compare comprehension and decision quality under gated versus ungated consent flows; field deployments can measure whether revocation clarity and outcome feedback reduce withdrawals due to uncertainty and improve sustained engagement. By aligning product increments with evaluative evidence, Consentio can scale dynamic consent in public-health research while preserving its ethical core.

These conclusions must nonetheless be interpreted in light of the study's limited scope. Because participants were primarily young, highly educated, and digitally proficient, the patterns reported here may not generalize to all populations. Scaling dynamic consent across diverse communities will require testing the recommended design features with broader cohorts, including those with varying levels of digital literacy and from different jurisdictions. Only through iterative evaluation in such diverse settings can we ensure that the socio-technical contract articulated here holds beyond the present context.

# 13 Thesis Contributions

The next sections will describe the work completed for this PhD thesis and summarize its relevance and contributions to the field of public health research over PHI.

### 13.1.1 Data Governance Framework Developed

An inter-organizational governance framework for public-health research that combines personal data sovereignty (PDS)(Pedro & Morita, 2022) with the Governance Analytical Framework (GAF)(Aeberhard & Rist, 2011; Hufty, 2008) was developed. The PDS stance explicitly centers data-subject control while acknowledging real-world power asymmetries and the need for concrete governance mechanisms not just "choice" to protect participants in multi-stakeholder settings.

Methodologically, five GAF elements were applied problem, actors, nodal points, social norms, and processes to map the domain. A scoping review identified core actors (data subjects, public-health researchers, IRBs, custodians/private companies, public entities), their collective problems and norms, and the transaction types that introduce authority or imbalance (e.g., directive vs. negotiated interactions). This mapping surfaced the decision arenas where governance must intervene to enable trustworthy data access and sharing.

To ground the framework in sector realities, we analysed the CIHI Health Data and Information Governance and Capability Framework, (Canadian Institutes of Health Research) and documented gaps for public-health research (e.g., over-emphasis on system performance over population health , limited cross-sector collaboration, weak community engagement, lack of strategy for emerging data types). These gaps motivated tailoring to public-health use-cases and informed stakeholder roles and controls in the developed model.

Further alignment with the framework ISO/IEC 38500 for governance responsibilities, Evaluate, Direct, Monitor and six supporting principles (Responsibility, Strategy, Acquisition, Performance, Conformance, Human Behaviour). This alignment provides a clear oversight cadence (evaluation metrics,

role assignment, and continuous monitoring) and a principled bridge from organizational policy to technical controls.

The resulting framework (Section 6) - (i) specifies actor responsibilities and nodal-point transactions, (ii) embeds Dynamic Informed Consent (DIC) to realize data-subject sovereignty, and (iii) explicitly aligns with GDPR duties to ensure lawful, transparent processing. The GAF Diagram presented in Section 6, show how standardized mechanisms can reduce power imbalances and streamline DSAs, improving researcher access to PHI while preserving participant rights.

### 13.1.2 Design and Architecture of the Dynamic Informed Consent Management Platform – Consentio

Guided by the governance model, we translated normative requirements into Consentio, a modular, policy-compliant Dynamic Informed Consent (DIC) platform. Section 7 purposefully "bridges" governance to code: every structural/relational requirement from Section 6 is decomposed into enforceable software controls, and every critical interaction is auditable.

Architectural goals and patterns: We implemented a layered architecture that (i) enforces role-segregation across stakeholders, (ii) isolates privacy-sensitive operations, and (iii) supports independent evolution of UI, orchestration, and compliance logic. The MVP implements core workflows study instantiation, consent issuance/revocation, participant messaging, audit queries and is containerized and deployed in Azure to support evaluation.

Ledger substrate and smart-contracts: Consent events are recorded on a private, permissioned Hyperledger Fabric network (v2.2). Fabric peers maintain the ledger and endorse transactions; orderers sequence them; a Certificate Authority issues identities; and channels isolate governance scopes (e.g., IRB-scoped review vs. study clusters). Chaincode encapsulates consent lifecycle logic with typed operations to create and query consent events (enroll, withdraw, revoke). All records are signed, time-stamped, and committed only when endorsement policies (including IRB peers) are satisfied.

This configuration operationalizes governance directive transactions are executed through smart-contracts; negotiation and reciprocity are supported via channel policy and transparent, role-limited visibility. The ledger provides the governance properties required in Section 6: transparency, auditability, real-time revocation, and decentralized trust. Technology Mapped (Governance into Technology Components) are presented in the table below:

*Table 25 - Technology mapped for the informed consent management platform.*

| # | Capability | Implementation / Details |
|---|---|---|
| 1 | Immutable audit trail | Hyperledger Fabric 2.x with endorsement by IRB peers before commits. |
| 2 | Segregated communications | Fabric private channels per study/actor set. |
| 3 | Real-time revocation | Fabric world-state + NodeJS event listeners. |
| 4 | Accessible UI | Angular 16 + Bootstrap (WCAG 2.1 AA). |
| 5 | Secure orchestration | Token-auth'd NodeJS (Express) microservices. |
| 6 | Policy-driven hosting | Azure App Service, Key Vault, Docker/Kubernetes; off-chain artifacts in SQL/Blob with on-chain integrity hashes. |
| 7 | Actor & use-case conformance | Platform roles map one-to-one to governance actors: Participants (data subjects), Researchers, PIs, IRB/Auditors, and Custodians, each with mandated interactions (e.g., "Grant/Revoke Consent," "Approve DC Form," "Validate Current Consent"). Cross-cutting concerns (Authenticate User, Log Action) are included in all critical flows to enforce RBAC and indelible audit logging. Pre/post-conditions encode regulatory invariants (e.g., quorum, revocation propagation). |
| 8 | Participant-facing modules | To reduce cognitive load and operationalize transparency mandates (e.g., TCPS2/GDPR), the UI includes a Study Grid and study-detail flow with a Consent Privacy Impact Quantification (CPIQ) gauge (0–100) that summarizes privacy risk/benefit and supports granular, informed decisions prior to enrollment. These modules instantiate the framework's transparency, autonomy, and risk-disclosure requirements at the point of use. |

Outcome (Aim 2 in brief). The delivered MVP demonstrates that a permissioned-ledger + microservices stack can enforce consent governance end-to-end without exposing PHI on-chain, while

making accountability and revocation verifiable to all authorized parties. This directly implements the framework developed in Section 6 and positions the platform for the Section 8 and 9 UX evaluation.

### 13.1.3 User Experience Evaluation

A mixed-methods user-experience evaluation was completed to assess Consentio after the platform was built. The evaluation used a pre/post design structured around validated instruments and open-ended feedback. A baseline profile of participants' digital ability and computer self-efficacy was captured using the Internet Skills Scale (ISS) and the Computer User Self-Efficacy (CUSE) scale, alongside demographics. After interacting with the platform, a post-use battery assessed perceived usability with the Post-Study System Usability Questionnaire (PSSUQ), overall satisfaction with a brief customer satisfaction questionnaire, and likelihood to recommend with a Net Promoter Score (NPS) item.

Instruments and scope were selected to provide complementary perspectives on user experience. PSSUQ (system usefulness, information quality, interface quality) was used for post-use usability; ISS profiled operational, navigation, social, creative, and mobile skills; CUSE profiled confidence in common computing tasks; the satisfaction questionnaire gathered concise ratings plus open-text suggestions; and NPS provided an advocacy signal. These instruments and their operational characteristics are documented within the study materials and are summarised in Sections 8 and 9.

To complement the surveys, a reflexive thematic analysis of the open-ended responses was conducted following Braun and Clarke's six-phase process (familiarisation, coding, theme development, review) (Braun & Clarke, 2006). Open-text inputs were compiled from the PSSUQ, customer-satisfaction questionnaire, NPS free-text prompt, and the demographics form; codes were generated (e.g., ease of use, centralised study management, filtering and layout preferences, notifications/help), clustered into themes, reviewed for fit, and narrated with representative quotations.

An extended triangulation linked qualitative themes to corresponding survey indicators to situate narrative patterns against quantitative signals (e.g., aligning comments about transparency, management

features, and usability with related PSSUQ, satisfaction, and NPS items). This triangulated view described in the qualitative section provides the structure for how the forthcoming results are organized and interpreted.

Data handling and analysis pipelines were prepared in Python (pandas/NumPy). For the quantitative surveys, item-level descriptives and scale-level summaries were computed. Categorical tallies were produced for satisfaction items; and standard Net Promoter Score (NPS) classification was applied. These procedures are detailed in Sections 8 and 9 analysis workflow; numerical results are presented in later sections.

Finally, to ensure that evaluation tasks reflected real use, the post-use survey and qualitative prompts were aligned with the platform's core, governance-aligned flows (e.g., viewing study information, granting/revoking consent, reviewing consent history and notifications) that are specified in the platform's use-case model from Section 7; this preserves traceability between the governance model, implemented features, and what was evaluated.

## References


Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. In *International Journal of Information Management* (Vol. 49, pp. 424–438). Elsevier Ltd. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Ackerman, J. L., & Proffit, W. R. (1995). Communication in orthodontic treatment planning: bioethical and informed consent issues. *The Angle Orthodontist*, *65*(4), 253–261. https://doi.org/10.1043/0003-3219(1995)065<0253:CIOTPB>2.0.CO;2

Aeberhard, A., & Rist, S. (2011). Investigating Policy Processes: The Governance Analytical Framework (GAF). *Ecological Economics*, *68*(4), 1171–1181. https://doi.org/10.1016/J.ECOLECON.2008.08.008

Ahmed, S. K., Mohammed, R. A., Nashwan, A. J., Ibrahim, R. H., Abdalla, A. Q., M. Ameen, B. M., & Khdhir, R. M. (2025). Using thematic analysis in qualitative research. *Journal of Medicine, Surgery, and Public Health*, *6*, 100198. https://doi.org/10.1016/J.GLMEDI.2025.100198

Aisyah, M., & Ruldeviyani, Y. (2019). Designing data governance structure based on data management body of knowledge (DMBOK) Framework: A case study on Indonesia deposit insurance corporation (IDIC). *2018 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2018*, 307–312. https://doi.org/10.1109/ICACSIS.2018.8618151

Ajunwa, I., Crawford, K., & Ford, J. S. (2016). Health and big data: An ethical framework for health information collection by corporate wellness programs. *Journal of Law, Medicine and Ethics*, *44*(3), 474–480. https://doi.org/10.1177/1073110516667943

Al-Badi, A., Tarhini, A., & Khan, A. I. (2018). Exploring big data governance frameworks. *Procedia Computer Science*, *141*, 271–277. https://doi.org/10.1016/j.procs.2018.10.181

Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. *Journal of Decision Systems*, *25*, 64–75. https://doi.org/10.1080/12460125.2016.1187397

Alhassan, I., Sammon, D., & Daly, M. (2019). Critical Success Factors for Data Governance: A Theory Building Approach. *Information Systems Management*, *36*(2), 98–110. https://doi.org/10.1080/10580530.2019.1589670

Allen, K. C., Whitfield, K., Rabinovich, R., & Sadruddin, S. (2021). The role of governance in implementing sustainable global health interventions: review of health system integration for integrated community case management (iCCM) of childhood illnesses. *BMJ Global Health*, *6*(3), e003257. https://doi.org/10.1136/BMJGH-2020-003257

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing 2018 23:5*, *23*(5), 839–859. https://doi.org/10.1007/S00779-017-1104-3

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, *23*(5–6), 839–859. https://doi.org/10.1007/s00779-017-1104-3

Amoako-Gyampah, K. (2004). ERP implementation factorsA comparison of managerial and end-user perspectives. *Business Process Management Journal*, *10*(2), 171–183. https://doi.org/10.1108/14637150410530244

Andersen, A., Yigzaw, K. Y., & Karlsen, R. (2014). Privacy preserving health data processing. *2014 IEEE 16th International Conference on E-Health Networking, Applications and Services, Healthcom 2014*, 225–230. https://doi.org/10.1109/HealthCom.2014.7001845

Anderson, K., Burford, O., & Emmerton, L. (2016). Mobile health apps to facilitate self-care: A qualitative study of user experiences. *PLoS ONE*, *11*(5), e0156164. https://doi.org/10.1371/journal.pone.0156164

Andrew Kirkpatrick, Joshue O Connor, Alastair Campbell, & Michael Cooper. (2025). *Web Content Accessibility Guidelines (WCAG) 2.1*. https://www.w3.org/TR/WCAG21/

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018a). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, *2018-Janua*. https://doi.org/10.1145/3190508.3190538

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018b). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, *2018-Janua*. https://doi.org/10.1145/3190508.3190538

Anomaly, J. (2011). Public health and public goods. *Public Health Ethics*, *4*(3), 251–259. https://doi.org/10.1093/PHE/PHR027

Appenzeller, A., Hornung, M., Kadow, T., Krempel, E., & Beyerer, J. (2022). Sovereign Digital Consent through Privacy Impact Quantification and Dynamic Consent. *Technologies 2022, Vol. 10, Page 35*, *10*(1), 35. https://doi.org/10.3390/TECHNOLOGIES10010035

Appenzeller, A., Kadow, T., Krempel, E., & Beyer, J. (2021). CPIQ - A Privacy Impact Quantification for Digital Medical Consent. *ACM International Conference Proceeding Series*, 534–543. https://doi.org/10.1145/3453892.3461653

Asaad, M., Habibullah, N. K., & Butler, C. E. (2020). The Impact of COVID-19 on Clinical Trials. *Annals of Surgery*, *272*(3), e222. https://doi.org/10.1097/SLA.0000000000004113

Asklund, I., Samuelsson, E., Hamberg, K., Umefjord, G., & Sjöström, M. (2019). User Experience of an App-Based Treatment for Stress Urinary Incontinence: Qualitative Interview Study. *J Med Internet Res 2019;21(3):E11296 Https://Www.Jmir.Org/2019/3/E11296*, *21*(3), e11296. https://doi.org/10.2196/11296

Assale, M., Barbero, E., & Cabitza, F. (2019). Digitizing the informed consent: The challenges to design for practices. *Proceedings - IEEE Symposium on Computer-Based Medical Systems*, *2019-June*, 609–615. https://doi.org/10.1109/CBMS.2019.00127

Association, W. M. (2013). World Medical Association Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects. *JAMA*, *310*(20), 2191–2194. https://doi.org/10.1001/JAMA.2013.281053

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 25–30. https://doi.org/10.1109/OBD.2016.11

Bagot, K. S., Matthews, S. A., Mason, M., Squeglia, L. M., Fowler, J., Gray, K., Herting, M., May, A., Colrain, I., Godino, J., Tapert, S., Brown, S., & Patrick, K. (2018). Current, future and potential use of mobile and wearable technologies and social media data in the ABCD study to increase understanding of contributors to child health. In *Developmental Cognitive Neuroscience* (Vol. 32, pp. 121–129). Elsevier Ltd. https://doi.org/10.1016/j.dcn.2018.03.008

Balan, S., Shristiraj, N., Shah, V., & Manjappa, A. (2017). Big data analysis of youth tobacco smoking trends in the United States. *Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017*, *2018-Janua*, 4727–4729. https://doi.org/10.1109/BIGDATA.2017.8258522

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, *52*(Volume 52, 2001), 1–26. https://doi.org/10.1146/ANNUREV.PSYCH.52.1.1/CITE/REFWORKS

Banerjee, S. (Sy), Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *Information Society*, *34*(1), 49–57. https://doi.org/10.1080/01972243.2017.1391912

Barney, J. R., & Antisdel, Michele. (2013). *Common Problems in Informed Consent*. https://your.yale.edu/policies-procedures/other/common-problems-informed-consent

Barrett, M. A., Humblet, O., Hiatt, R. A., & Adler, N. E. (2013). Big Data and Disease Prevention: From Quantified Self to Quantified Communities. In *Big Data* (Vol. 1, Number 3, pp. 168–175). Mary Ann Liebert Inc. https://doi.org/10.1089/big.2013.0027

Belli, L., Gaspar, W. B., & Singh Jaswant, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law and Security Review*, *54*. https://doi.org/10.1016/j.clsr.2024.106017

Benchoufi, M., Porcher, R., & Ravaud, P. (2018). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research*, *6*, 66. https://doi.org/10.12688/f1000research.10531.5

Benchoufi, M., & Ravaud, P. (2017a). Blockchain technology for improving clinical research quality. In *Trials* (Vol. 18, Number 1, p. 335). BioMed Central Ltd. https://doi.org/10.1186/s13063-017-2035-z

Benchoufi, M., & Ravaud, P. (2017b). Blockchain technology for improving clinical research quality. In *Trials* (Vol. 18, Number 1). BioMed Central Ltd. https://doi.org/10.1186/s13063-017-2035-z

Benke, K., & Benke, G. (2018). Artificial intelligence and big data in public health. *International Journal of Environmental Research and Public Health*, *15*(12). https://doi.org/10.3390/ijerph15122796

Bernstein, J. (2022). Not the Last Word: Primum Non Nocere Is Harmful. Primum Noce Apte May Help. *Clinical Orthopaedics and Related Research*, *481*(2), 211. https://doi.org/10.1097/CORR.0000000000002509

Bester, J., Cole, C. M., & Kodish, E. (2016). The limits of informed consent for an overwhelmed patient: Clinicians' role in protecting patients and preventing overwhelm. *AMA Journal of Ethics*, *18*(9), 869–886. https://doi.org/10.1001/JOURNALOFETHICS.2016.18.9.PEER2-1609

Biros, M. (2018). Capacity, Vulnerability, and Informed Consent for Research. *Journal of Law, Medicine & Ethics*, *46*(1), 72–78. https://doi.org/10.1177/1073110518766021

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere - A use-case of blockchains in the pharma supply-chain. *Proceedings of the IM 2017 - 2017 IFIP/IEEE International*

*Symposium on Integrated Network and Service Management*, 772–777. https://doi.org/10.23919/INM.2017.7987376

Brandt, A. M. (1978). Racism and Research: The Case of the Tuskegee Syphilis Study. *The Hastings Center Report*, *8*(6), 21. https://doi.org/10.2307/3561468

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706QP063OA

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, *18*(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238

Braun, V., & Clarke, V. (2022). Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher. *International Journal of Transgender Health*, *24*(1), 1. https://doi.org/10.1080/26895269.2022.2129597

Braun, V., & Clarke, V. (2024a). A critical review of the reporting of reflexive thematic analysis in Health Promotion International. *Health Promotion International*, *39*(3), 49. https://doi.org/10.1093/HEAPRO/DAAE049

Braun, V., & Clarke, V. (2024b). Supporting best practice in reflexive thematic analysis reporting in Palliative Medicine: A review of published research and introduction to the Reflexive Thematic Analysis Reporting Guidelines (RTARG). *Palliative Medicine*, *38*(6), 608–616. https://doi.org/10.1177/02692163241234800/SUPPL_FILE/SJ-PDF-1-PMJ-10.1177_02692163241234800.PDF

Braun, V., Clarke, V., Hayfield, N., Davey, L., & Jenkinson, E. (2022). Doing Reflexive Thematic Analysis. *Supporting Research in Counselling and Psychotherapy: Qualitative, Quantitative, and Mixed Methods Research*, 19–38. https://doi.org/10.1007/978-3-031-13942-0_2

Brinkmann, S. , & K. S. (2015a). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE Publications, Inc.

Brinkmann, S. , & K. S. (2015b). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE Publications, Inc .

Broek, T. van den, & Veenstra, A. F. van. (2015). *Modes of Governance in Inter-Organizational Data Collaborations*. 0–12. https://doi.org/10.18151/7217509

Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S., & Nadeau, E. (2017). *An introduction to privacy engineering and risk management in federal systems*. https://doi.org/10.6028/NIST.IR.8062

Bublitz, F. M., Oetomo, A., Sahu, K. S., Kuang, A., Fadrique, L. X., Velmovitsky, P. E., Nobrega, R. M., & Morita, P. P. (2019). Disruptive technologies for environment and health research: An overview of artificial intelligence, blockchain, and internet of things. *International Journal of Environmental Research and Public Health*, *16*(20), 16, 3847. https://doi.org/10.3390/ijerph16203847

Budin-Ljøsne, I., Teare, H. J. A., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., Collett, C., D'Abramo, F., Felzmann, H., Finlay, T., Javaid, M. K., Jones, E., Katić, V., Simpson, A., & Mascalzoni, D. (2017). Dynamic Consent: A potential solution to some of the challenges of modern biomedical research. *BMC Medical Ethics*, *18*(1), 4. https://doi.org/10.1186/s12910-016-0162-9

Buterin, V. (2013). *Ethereum Whitepaper | Ethereum.org*. Ethereum.Org. https://ethereum.org/en/whitepaper/

Cai, L., & Zhu, Y. (2015). The Challenges of Data Quality and Data Quality Assessment in the Big Data Era. *Data Science Journal*, *14*(0). https://doi.org/10.5334/DSJ-2015-002

Calder, A. (2019). *ISO/IEC 38500: A pocket guide, second edition*. https://learning-oreilly-com.proxy.lib.uwaterloo.ca/library/view/iso-iec-38500-a/9781787781702/

Campbell, K. A., Orr, E., Durepos, P., Nguyen, L., Li, L., Whitmore, C., Gehrke, P., Graham, L., & Jack, S. M. (2021). Reflexive Thematic Analysis for Applied Qualitative Health Research. *The Qualitative Report*, *26*(6), 2011–2028. https://doi.org/10.46743/2160-3715/2021.5010

Canadian Institute for Health Information. (2020). *CIHI's Health Data and Information Governance and Capability Framework*.

Canadian Institutes of Health Research. (2026a). *Health data and information governance and capability framework | CIHI*. https://www.cihi.ca/en/health-data-and-information-governance-and-capability-framework

Canadian Institutes of Health Research. (2026b). *Welcome to the Canadian Institutes of Health Research - CIHR*. https://cihr-irsc.gc.ca/e/193.html

Canadian Institutes of Health Research, N. S. and E. R. C. of C. & S. S. and H. R. C. (2022). *TCPS 2 (2022) – Chapter 3: The Consent Process*. https://ethics.gc.ca/eng/tcps2-eptc2_2022_chapter3-chapitre3.html

Cassidy, S., & Eachus, P. (2002). Developing the Computer User Self-Efficacy (Cuse) Scale: Investigating the Relationship between Computer Self-Efficacy, Gender and Experience with Computers. *Http://Dx.Doi.Org/10.2190/JGJR-0KVL-HRF7-GCNV*, *26*(2), 133–153. https://doi.org/10.2190/JGJR-0KVL-HRF7-GCNV

*Chaincode for Developers — hyperledger-fabricdocs master documentation*. (n.d.). Retrieved May 23, 2020, from https://hyperledger-fabric.readthedocs.io/en/latest/chaincode4ade.html?highlight=chaincode.

Chen, M., Hao, Y., Hwang, K., Wang, Lin, & Wang, Lu. (2017). Disease Prediction by Machine Learning over Big Data from Healthcare Communities. *IEEE Access*, *5*, 8869–8879. https://doi.org/10.1109/ACCESS.2017.2694446

Cheng, G., Li, Y., Gao, Z., & Liu, X. (2018). Cloud data governance maturity model. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, *2017-Novem*, 517–520. https://doi.org/10.1109/ICSESS.2017.8342968

Chua, P. H. T., Li, Y., & He, W. (2019, May 21). Adopting hyperledger fabric blockchain for EPCglobal network. *2019 IEEE International Conference on RFID, RFID 2019*. https://doi.org/10.1109/RFID.2019.8719271

CIO Central Guest. (2017). *He Who Rules The Data, Rules The World: A Brief History Of Data Governance*. https://www.forbes.com/sites/ciocentral/2017/11/16/he-who-rules-the-data-rules-the-world-a-brief-history-of-data-governance/?sh=fc1b0e739b57

Cocanour, C. S. (2017). Informed consent—It's more than a signature on a piece of paper. *The American Journal of Surgery*, *214*(6), 993–997. https://doi.org/10.1016/J.AMJSURG.2017.09.015

Coe, A., Paquet, G., & Roy, J. (2001). E-governance and smart communities: A social learning challenge. In *Social Science Computer Review* (Vol. 19, Number 1). https://doi.org/10.1177/089443930101900107

Cosman, D. (2023). The Nuremberg Code on Human Experimentation. A Historical Overview. *Romanian Journal of Artistic Creativity*, *11*(2), 3–14.

Dankar, F. K., Gergely, M., Malin, B., Badji, R., Dankar, S. K., & Shuaib, K. (2020). Dynamic-informed consent: A potential solution for ethical dilemmas in population sequencing initiatives. *Computational and Structural Biotechnology Journal*, *18*, 913–921. https://doi.org/10.1016/J.CSBJ.2020.03.027

de Andrade Cardieri, G., & Zaina, L. M. (2018). Analyzing user experience in mobile web, native and progressive web applications: A user and HCI specialist perspectives. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3274192.3274201

De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. In *Library Review* (Vol. 65, Number 3, pp. 122–135). Emerald Group Publishing Ltd. https://doi.org/10.1108/LR-06-2015-0061

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family Medicine and Community Health*, *7*(2), 57. https://doi.org/10.1136/FMCH-2018-000057

Demchenko, Y., De Laat, C., & Membrey, P. (2014). Defining architecture components of the Big Data Ecosystem. *2014 International Conference on Collaboration Technologies and Systems, CTS 2014*, 104–112. https://doi.org/10.1109/CTS.2014.6867550

Digital Inclusion Index. (2021). *Case study: Taking a deep dive into Digital Ability*. https://digitalinclusionindex.org.au/case-study-taking-a-deep-dive-into-digital-ability/

Dobson, R., Wihongi, H., & Whittaker, R. (2023). Exploring patient perspectives on the secondary use of their personal health information: an interview study. *BMC Medical Informatics and Decision Making*, *23*(1), 66. https://doi.org/10.1186/S12911-023-02143-1/FIGURES/1

Drogt, J., Milota, M., Vos, S., Bredenoord, A., & Jongsma, K. (2022). Integrating artificial intelligence in pathology: a qualitative interview study of users' experiences and expectations. *Modern Pathology*, *35*(11), 1540–1550. https://doi.org/10.1038/S41379-022-01123-6

Drutskoy, D., Keller, E., & Rexford, J. (2013). Scalable network virtualization in software-defined networks. *IEEE Internet Computing*, *17*(2), 20–27. https://doi.org/10.1109/MIC.2012.144

Epstein, R. L. (1990). *The Semantic Foundations of Logic Volume 1: Propositional Logics* (Vol. 35). Springer Netherlands. https://doi.org/10.1007/978-94-009-0525-2

Eslami Andargoli, A., Scheepers, H., Rajendran, D., & Sohal, A. (2017). Health information systems evaluation frameworks: A systematic review. *International Journal of Medical Informatics*, *97*, 195–209. https://doi.org/10.1016/j.ijmedinf.2016.10.008

European Parliament and Council of the European Union. (2016a). *Art. 12 GDPR – Transparent information, communication and modalities for the exercise of the rights of the data subject*. https://gdpr-info.eu/art-12-gdpr/

European Parliament and Council of the European Union. (2016b). *Art. 13 GDPR – Information to be provided where personal data is collected from the data subject*. https://gdpr-info.eu/art-13-gdpr/

European Parliament and Council of the European Union. (2016c). *Art. 14 GDPR – Information to be provided where personal data have not been obtained from the data subject*. https://gdpr-info.eu/art-14-gdpr/

European Parliament and Council of the European Union. (2016d). *Art. 35 GDPR – Data protection impact assessment*. https://gdpr-info.eu/art-35-gdpr/

European Parliament and Council of the European Union. (2016e). *Art. 89 GDPR – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*. https://gdpr-info.eu/art-89-gdpr/

European Parliament and Council of the European Union. (2016f). *Chapter 3 – Rights of the data subject | General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/chapter-3/

European Parliament and Council of the European Union. (2016g). *Data Protection Impact Assessment (DPIA)*. https://gdpr.eu/data-protection-impact-assessment-template/

European Parliament and of the Council of 27 April 2016. (2016). *Regulation - 2016/679 - EN - gdpr - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

Evren, E., Uri, G., Valliappa, L., Anita, K.-G., & Jessi, A. (2021). *1. What Is Data Governance? | Data Governance: The Definitive Guide*. https://learning.oreilly.com/library/view/data-governance-the/9781492063483/ch01.html

Fadrique, L. X. (2019). *Privacy and Trust in Healthcare IoT Data Sharing: A Snapshot of the Users' Perspectives* [University of Waterloo]. https://uwspace.uwaterloo.ca/handle/10012/15333

Falessi, D., Babar, A., Cantone, M., & Kruchten, G. (2010). Applying Empirical Software Engineering to Software Architecture: Challenges and Lessons Learned. In *Empirical Software Engineering Journal* (Vol. 15, Number 3).

Fatema, K., Hadziselimovic, E., Pandit, H., Debruyne, C., Lewis, D., & O'Sullivan, D. (2017). Compliance through informed consent: Semantic based consent permission and data management model. In *CEUR Workshop Proceedings* (Vol. 1951). CEUR-WS.

Firouzi, F., Rahmani, A. M., Mankodiya, K., Badaroglu, M., Merrett, G. V., Wong, P., & Farahani, B. (2018). Internet-of-Things and big data for smarter healthcare: From device to architecture, applications and analytics. *Future Generation Computer Systems*, *78*, 583–586. https://doi.org/10.1016/J.FUTURE.2017.09.016

Fisher, N. I., & Kordupleski, R. E. (2019). Good and bad market research: A critical review of Net Promoter Score. *Applied Stochastic Models in Business and Industry*, *35*(1), 138–151. https://doi.org/10.1002/ASMB.2417

Frank, J., & Di Ruggiero, E. (2003). Public health in Canada: What are the real issues? In *Canadian Journal of Public Health* (Vol. 94, Number 3). https://doi.org/10.1007/bf03405064

Funnell, E. L., Spadaro, B., Martin-Key, N., Metcalfe, T., & Bahn, S. (2022). mHealth Solutions for Mental Health Screening and Diagnosis: A Review of App User Perspectives Using Sentiment and Thematic Analysis. *Frontiers in Psychiatry*, *13*, 857304. https://doi.org/10.3389/FPSYT.2022.857304/BIBTEX

Gamache, R., Kharrazi, H., & Weiner, J. P. (2018). Public and Population Health Informatics: The Bridging of Big Data to Benefit Communities. *Yearbook of Medical Informatics*, *27*(1), 199–206. https://doi.org/10.1055/S-0038-1667081/ID/JRGAMACHE-71

Github, R. (2019). *Glossary — hyperledger-fabricdocs master documentation*. https://hyperledger-fabric.readthedocs.io/en/latest/glossary.html?highlight=%22leading peer%22#leading-peer

Gómez-Barroso, J.-L., Feijóo, C., & Martínez-Martínez, I. J. (2018). Privacy calculus: Factors that influence the perception of benefit. *El Profesional de La Información*, *27*(2), 341. https://doi.org/10.3145/epi.2018.mar.12

Gonzalez, G., Vaculik, K., Khalil, C., Zektser, Y., Arnold, C., Almario, C. V., Spiegel, B., & Anger, J. (2022). Using Large-scale Social Media Analytics to Understand Patient Perspectives About Urinary Tract Infections: Thematic Analysis. *J Med Internet Res 2022;24(1):E26781 Https://Www.Jmir.Org/2022/1/E26781*, *24*(1), e26781. https://doi.org/10.2196/26781

Google Inc. (2022). *COVID-19 Community Mobility Reports*. https://www.google.com/covid19/mobility/

Google Inc. (2026). *Angular.io*. https://angular.io/

Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2019). FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second. *ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*, 455–463. https://doi.org/10.1109/BLOC.2019.8751452

Government of Canada. (2019a). *About the Agency - Canada.ca*. https://www.canada.ca/en/public-health/corporate/mandate/about-agency.html

Government of Canada. (2019b). *Requirements for Informed Consent Documents - Canada.ca*. https://www.canada.ca/en/health-canada/services/science-research/science-advice-decision-making/research-ethics-board/requirements-informed-consent-documents.html

Grady, C., Cummings, S. R., Rowbotham, M. C., McConnell, M. V., Ashley, E. A., & Kang, G. (2017). Informed Consent. *New England Journal of Medicine*, *376*(9), 856–867. https://doi.org/10.1056/NEJMra1603773

Graña Possamai, C., Ravaud, P., Ghosn, L., & Tran, V. T. (2020). Use of wearable biometric monitoring devices to measure outcomes in randomized clinical trials: a methodological systematic review. *BMC Medicine*, *18*(1). https://doi.org/10.1186/s12916-020-01773-w

Greenspan, G. (2015). MultiChain Private Blockchain - White Paper. In *White Paper*. https://doi.org/10.1053/sonc.2002.32894

Gregory, A. (2011a). Data governance Protecting and unleashing the value of your customer data assets: Stage 1: Understanding data governance and your current data management capability. *Journal of Direct, Data and Digital Marketing Practice*, *12*(3), 230–248. https://doi.org/10.1057/dddmp.2010.41

Gregory, A. (2011b). Data governance Protecting and unleashing the value of your customer data assets: Stage 1: Understanding data governance and your current data management capability. *Journal of Direct, Data and Digital Marketing Practice*, *12*(3), 230–248. https://doi.org/10.1057/DDDMP.2010.41/FIGURES/7

Grishin, D., Obbad, K., Estep, P., Cifric, M., Zhao, Y., & Church, G. (2018). Blockchain-enabled genomic data sharing and analysis platform. In *Nebular Genomics*.

Guegan, D. (2017). Public Blockchain versus Private blockhain. In *Documents de travail du Centre d'Economie de la Sorbonne*. http://centredeconomiesorbonne.univ-paris1.fr/%0Ahttps://halshs.archives-ouvertes.fr/halshs-01524440

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough? *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Hande, S. A., & Mane, S. B. (2015). An analysis on data Accountability and Security in cloud. *2015 International Conference on Industrial Instrumentation and Control, ICIC 2015*, 713–717. https://doi.org/10.1109/IIC.2015.7150835

Hargittai, E., & Dobransky, K. (2017). Old dogs, new clicks: Digital inequality in skills and uses among older adults. *Canadian Journal of Communication*, *42*(2), 195–212. https://doi.org/10.22230/CJC.2017V42N2A3176/ASSET/IMAGES/CJC.2017V42N2A3176-T5B.PNG

Hargittai, E., Piper, A. M., & Morris, M. R. (2019). From internet access to internet skills: digital inequality among older adults. *Universal Access in the Information Society*, *18*(4), 881–890. https://doi.org/10.1007/S10209-018-0617-5/METRICS

Health Canada. (2021). *Annex 11 to the good manufacturing practices guide: Computerized Systems*. https://www.canada.ca/en/health-canada/services/drugs-health-products/compliance-enforcement/good-manufacturing-practices/guidance-documents/annex-11-guide-computerized-systems-gui-0050.html

Health Level Seven International. (2020). *Overview - FHIR v4.0.1*. http://hl7.org/fhir/overview.html

Heinold, E., Rosen, P. H., & Wischniewski, S. (2025). Usability Questionnaire for Robotic Systems Based on the ISO 9241-110. *IEEE Robotics and Automation Letters*, *10*(3), 2231–2238. https://doi.org/10.1109/LRA.2025.3526557

Helliwell, J. R., & Massera, C. (2022). The four Rs and crystal structure analysis: reliability, reproducibility, replicability and reusability. *Journal of Applied Crystallography*, *55*(Pt 5), 1351–1358. https://doi.org/10.1107/S1600576722007208

Henning, M. (2007). API design matters. In *Queue* (Vol. 5, Number 4, pp. 24–36). https://doi.org/10.1145/1255421.1255422

Hensen, B., Mackworth-Young, C. R. S., Simwinga, M., Abdelmagid, N., Banda, J., Mavodza, C., Doyle, A. M., Bonell, C., & Weiss, H. A. (2021). Remote data collection for public health research in a COVID-19 era: ethical implications, challenges and opportunities. *Health Policy and Planning*, *36*(3), 360–368. https://doi.org/10.1093/HEAPOL/CZAA158

Holmes, J. H., Elliott, T. E., Brown, J. S., Raebel, M. A., Davidson, A., Nelson, A. F., Chung, A., La Chance, P., & Steiner, J. F. (2014). Clinical research data warehouse governance for distributed research networks in the USA: a systematic review of the literature. *Journal of the American Medical Informatics Association*, *21*(4), 730–736. https://doi.org/10.1136/AMIAJNL-2013-002370

Horton, R., Beaglehole, R., Bonita, R., Raeburn, J., McKee, M., & Wall, S. (2014). From public to planetary health: A manifesto. In *The Lancet* (Vol. 383, Number 9920). https://doi.org/10.1016/S0140-6736(14)60409-8

Hosseini Teshnizi, S., Hayavi Haghighi, M. H., & Alipour, J. (2021). Evaluation of health information systems with ISO 9241-10 standard: A systematic review and meta-analysis. *Informatics in Medicine Unlocked*, *25*, 100639. https://doi.org/10.1016/J.IMU.2021.100639

Hufty, M. (2008). *The Governance Analytical Framework*.

*hydrachain/hc_consensus_explained.md at develop · HydraChain/hydrachain · GitHub*. (n.d.). Retrieved May 23, 2020, from https://github.com/HydraChain/hydrachain/blob/develop/hc_consensus_explained.md

Hyperledger. (2019a). *Blockchain network — hyperledger-fabricdocs master documentation*. https://hyperledger-fabric.readthedocs.io/en/latest/network/network.html#

Hyperledger. (2019b). *The Ordering Service — hyperledger-fabricdocs master documentation*. https://hyperledger-fabric.readthedocs.io/en/release-2.0/orderer/ordering_service.html

Hyperledger Foundation. (2026a). *Hyperledger Fabric*. https://www.hyperledger.org/projects/fabric

Hyperledger Foundation. (2026b). *Hyperledger Fabric Network*. tps://hyperledger-fabric.readthedocs.io/en/release-1.2/network/network.html#defining-a-consortium.

Hyperledger Foundation. (2026c). *Hyperledger Fabric SDK for Node.js*. https://hyperledger.github.io/fabric-sdk-node/release-1.4/Client.html

HyperledgerDocs. (2018). *Introduction — hyperledger-fabricdocs master documentation*. Hyperledger-Fabric.Readthedocs.Io. https://doi.org/10.2320/matertrans.47.1898

IBM. (2018). *IBM White Paper: Blockchain and GDPR*. *1*(1), 6.

IBM. (2020). *IBM Blockchain Platform - IBM Blockchain | IBM*. https://www.ibm.com/blockchain/platform%0Attps://www.ibm.com/blockchain/platform

ISO. (2019). *ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*.

ISO/IEC. (2018). *ISO 9241-11:2018(en), Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*. Iso. https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en

Jaiman, V., & Urovi, V. (2020). A Consent Model for Blockchain-Based Health Data Sharing Platforms. *IEEE Access*, *8*, 143734–143745. https://doi.org/10.1109/ACCESS.2020.3014565

Jakob Nielsen. (2006). *F-Shaped Pattern For Reading Web Content (original eyetracking research) - NN/G*. https://www.nngroup.com/articles/f-shaped-pattern-reading-web-content-discovered/

Jakob Nielsen. (2024). *10 Usability Heuristics for User Interface Design - NN/G*. https://www.nngroup.com/articles/ten-usability-heuristics/

John, L. (2018). *The Seven Simple Principles of Health Care Data Governance*. https://www.advisory.com/topics/information-security/2018/04/the-seven-simple-principles-of-health-care-data-governance

Jones, D. S., Grady, C., & Lederer, S. E. (2016). "Ethics and Clinical Research" — The 50th Anniversary of Beecher's Bombshell. *New England Journal of Medicine*, *374*(24), 2393–2398. https://doi.org/10.1056/NEJMMS1603756/SUPPL_FILE/NEJMMS1603756_DISCLOSURES.PDF

Jones, M., Johnson, M., Shervey, M., Dudley, J. T., & Zimmerman, N. (2019). Privacy-preserving methods for feature engineering using blockchain: Review, evaluation, and proof-of-concept. *Journal of Medical Internet Research*, *21*(8), e13600. https://doi.org/10.2196/13600

Jurkovic, R., & Kopal, R. (2025). Self-Assessment of Digital Literacy Skills Using Internet Skills Scale (ISS): A Preliminary Report. *2025 MIPRO 48th ICT and Electronics Convention*, 1007–1012. https://doi.org/10.1109/MIPRO65660.2025.11131720

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). A Systematic Review of Blockchain for Consent Management. *Healthcare*, *9*(2), 137. https://doi.org/10.3390/healthcare9020137

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/JAN.13031

Katal, A., Wazid, M., & Goudar, R. H. (2013). Big data: Issues, challenges, tools and Good practices. *2013 6th International Conference on Contemporary Computing, IC3 2013*, 404–409. https://doi.org/10.1109/IC3.2013.6612229

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2014). Dynamic consent: a patient interface for twenty-first century research networks. *European Journal of Human Genetics*, *23*(2), 141. https://doi.org/10.1038/EJHG.2014.71

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015a). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics*, *23*(2), 141–146. https://doi.org/10.1038/ejhg.2014.71

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015b). Dynamic consent: a patient interface for twenty-first century research networks. *European Journal of Human Genetics : EJHG*, *23*(2), 141–146. https://doi.org/10.1038/EJHG.2014.71

Kelley, K., & Pornprasertmanit, S. (2016). Confidence intervals for population reliability coefficients: Evaluation of methods, recommendations, and software for composite measures. *Psychological Methods*, *21*(1), 69–92. https://doi.org/10.1037/A0040086

Kerpel-Fronius, S., Becker, S., Barrett, J., Brun, J., Carlesi, R., Chan, A., Collia, L. F., Dubois, D. J., Kleist, P., Koski, G., Kurihara, C., Laranjeira, L. F., Schenk, J., & Silva, H. (2018). The shared ethical responsibility of medically and non-medically qualified experts in human drug development teams. *Frontiers in Pharmacology*, *9*(SEP), 843. https://doi.org/10.3389/FPHAR.2018.00843/FULL

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148–152. https://doi.org/10.1145/1629175.1629210

Khokhar, R. H., Chen, R., Fung, B. C. M., & Lui, S. M. (2014). Quantifying the costs and benefits of privacy-preserving health data publishing. *Journal of Biomedical Informatics*, *50*, 107–121. https://doi.org/10.1016/J.JBI.2014.04.012

Khoury, M. J., & Ioannidis, J. P. A. (2014). Big data meets public health. In *Science* (Vol. 346, Number 6213, pp. 1054–1055). Science. https://doi.org/10.1126/science.aaa2709

Kim, H. Y., & Cho, J. S. (2018). Data governance framework for big data implementation with NPS Case Analysis in Korea. *Journal of Business and Retail Management Research*, *12*(3), 36–46. https://doi.org/10.24052/jbrmr/v12is03/art-04

Kim, K. K., Browe, D. K., Logan, H. C., Holm, R., Hack, L., & Ohno-Machado, L. (2014). Data governance requirements for distributed clinical research networks: triangulating perspectives of diverse stakeholders. *Journal of the American Medical Informatics Association : JAMIA*, *21*(4), 714–719. https://doi.org/10.1136/amiajnl-2013-002308

Knifed, E., Lipsman, N., Mason, W., & Bernstein, M. (2008). Patients' perception of the informed consent process for neurooncology clinical trials. *Neuro-Oncology*, *10*(3), 348–354. https://doi.org/10.1215/15228517-2008-007

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences of the United States of America*, *111*(24), 8788–8790. https://doi.org/10.1073/pnas.1320040111

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association : JAMIA*, *24*(6), 1211–1220. https://doi.org/10.1093/JAMIA/OCX068

L Marelli, G. T. (2018). Scrutinizing the EU general data protection regulation. *Science*, *360*(6388), 496–498. https://doi.org/10.1126/science.aar5419

Lange, C. F. J., Chaudron, M. R. V., & Muskens, J. (2006). In practice: UML software architecture and design description. *IEEE Software*, *23*(2), 40–46. https://doi.org/10.1109/MS.2006.50

Laplante, P. A., & Laplante, N. (2016). The Internet of Things in Healthcare: Potential Applications and Challenges. *IT Professional*, *18*(3), 2–4. https://doi.org/10.1109/MITP.2016.42

Lewis, J. R. (2011). Psychometric Evaluation of the PSSUQ Using Data from Five Years of Usability Studies. *Http://Dx.Doi.Org/10.1080/10447318.2002.9669130*, *14*(3–4), 463–488. https://doi.org/10.1080/10447318.2002.9669130

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, *88*, 8–17. https://doi.org/10.1016/j.ijmedinf.2015.12.010

Li, Q., Lan, L., Zeng, N., You, L., Yin, J., Zhou, X., & Meng, Q. (2019). A Framework for Big Data Governance to Advance RHINs: A Case Study of China. *IEEE Access*, *7*, 50330–50338. https://doi.org/10.1109/ACCESS.2019.2910838

Litton, J.-E. (2017). We must urgently clarify data-sharing rules. *Nature*, *541*(7638), 437. https://doi.org/10.1038/541437a

Lo, Y. S., Yang, C. Y., Chien, H. F., Chang, S. S., Lu, C. Y., & Chen, R. J. (2019). Blockchain-Enabled iWellChain Framework Integration With the National Medical Referral System: Development and Usability Study. *Journal of Medical Internet Research*, *21*(12). https://doi.org/10.2196/13563

Loftus, J. R., Russell, C., Kusner, M. J., & Silva, R. (2018). *Causal Reasoning for Algorithmic Fairness*. https://arxiv.org/abs/1805.05859v1

Lopez, A. D. (2010). Sharing data for public health: where is the vision? *Bull World Health Organ*, *88*(6), 467. https://doi.org/10.2471/blt.10.078956

Mamo, N., Martin, G. M., Desira, M., Ellul, B., & Ebejer, J. P. (2020). Dwarna: a blockchain solution for dynamic consent in biobanking. *European Journal of Human Genetics*, *28*(5), 609–626. https://doi.org/10.1038/s41431-019-0560-9

Mannonen, P., Aikala, M., Koskinen, H., & Savioja, P. (2014). Uncovering the user experience with critical experience interviews. *Proceedings of the 26th Australian Computer-Human Interaction Conference, OzCHI 2014*, 452–455. https://doi.org/10.1145/2686612.2686684

Marelli, L., Lievevrouw, E., & Van Hoyweghen, I. (2020). Fit for purpose? The GDPR and the governance of European digital health. *Policy Studies*, *41*(5), 447–467. https://doi.org/10.1080/01442872.2020.1724929

Marelli, L., & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation. *Science*, *360*(6388), 496–498. https://doi.org/10.1126/SCIENCE.AAR5419

Martin-Sanchez, F. J., Aguiar-Pulido, V., Lopez-Campos, G. H., Peek, N., & Sacchi, L. (2017). Secondary Use and Analysis of Big Data Collected for Patient Care. *Yearbook of Medical Informatics*, *26*(1), 28–37. https://doi.org/10.15265/IY-2017-008/ID/JR008-65

Mascalzoni, D., Melotti, R., Pattaro, C., Pramstaller, P. P., Gögele, M., De Grandi, A., & Biasiotto, R. (2022). Ten years of dynamic consent in the CHRIS study: informed consent as a dynamic process. *European Journal of Human Genetics 2022*, 1–7. https://doi.org/10.1038/s41431-022-01160-4

Mathew, A. (2024). *Industry News 2024 Cloud Data Sovereignty Governance and Risk Implications of Cross Border Cloud Storage*. https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage

Mcconaghy, Trent, Marques, R., Müller, A., De Jonghe, D., Mcconaghy, Troy, Mcmullen, G., Henderson, R., Bellemare, S., & Granzotto, A. (2016). BigchainDB: A Scalable Blockchain Database (DRAFT). In *BigchainDB*.

McDonald, M. (2022). The Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans. In *eweb:194010*.

McGinn, C. A., Grenier, S., Duplantie, J., Shaw, N., Sicotte, C., Mathieu, L., Leduc, Y., Légaré, F., & Gagnon, M. P. (2011). Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records: A systematic review. *BMC Medicine*, *9*(1), 1–10. https://doi.org/10.1186/1741-7015-9-46/TABLES/1

McMahon, A., Buyx, A., & Prainsack, B. (2019). Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond. *Medical Law Review*, *28*(1), 155–182. https://doi.org/10.1093/medlaw/fwz016

McNamara, D. S. (2013). The epistemic stance between the author and reader: A driving force in the cohesion of text and writing. *Discourse Studies*, *15*(5), 579–595. https://doi.org/10.1177/1461445613501446

*Membership — hyperledger-fabricdocs master documentation*. (n.d.). Retrieved May 23, 2020, from https://hyperledger-fabric.readthedocs.io/en/release-1.4/membership/membership.html?highlight=network membership updates

*Membership Service Provider (MSP) — hyperledger-fabricdocs master documentation*. (n.d.). Retrieved May 23, 2020, from https://hyperledger-fabric.readthedocs.io/en/latest/membership/membership.html

Micheli, M, Ponti, M., Craglia, M., & Suman, A. B. (2020). Emerging models of data governance. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720948087

Micheli, Marina, Ponti, M., Craglia, M., & Suman, A. B. (2020). Emerging models of data governance in the age of datafication: *Https://Doi.Org/10.1177/2053951720948087*, *7*(2). https://doi.org/10.1177/2053951720948087

Microsoft Learn. (2026). *Saga Design Pattern - Azure Architecture Center | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/architecture/patterns/saga?utm_source=chatgpt.com

Miranda, P. A., Kaur, J., & Morita, P. (2023). UbiSecE: UbiLab's Secure Cloud Environment for Public Health Research in Microsoft Azure. *International Conference on Wireless and Mobile Computing, Networking and Communications*, *2023-June*, 1–4. https://doi.org/10.1109/WIMOB58348.2023.10187831

Mowat, D. L., & Butler-Jones, D. (2007). Public health in Canada: a difficult history. *HealthcarePapers*, *7*(3), 31–36. https://doi.org/10.12927/hcpap..18755

MRCT Center. (2016). *Designing impactful informed consent processes that empower participants*. https://mrctcenter.org/resource/2016-mrct-center-progress-report/

MRCT Center. (2022). *The Multi-Regional Clinical Trials Center of Brigham and Women's Hospital and Harvard*. https://mrctcenter.org/resource/2022-mrct-center-impact-report/

MRCT Center. (2024). *Designing Impactful Informed Consent Processes that Empower Participants*. https://mrctcenter.org/resource/designing-impactful-informed-consent-processes-that-empower-participants/

Murphy, C. A., Coover, D., & Owen, S. V. (1989). Development and Validation of the Computer Self-Efficacy Scale. *Http://Dx.Doi.Org/10.1177/001316448904900412*, *49*(4), 893–899. https://doi.org/10.1177/001316448904900412

Musmade, P., Nijhawan, L., Udupa, N., Bairy, K., Bhat, K., Janodia, M., & Muddukrishna, B. (2013). Informed consent: Issues and challenges. *Journal of Advanced Pharmaceutical Technology & Research*, *4*(3), 134. https://doi.org/10.4103/2231-4040.116779

Nadanyiova, M., Gajanova, L., & Baquero, A. (2022). Net Promoter Score (NPS) and Customer Satisfaction: Relationship and Efficient Management. *Sustainability 2022, Vol. 14, Page 2011*, *14*(4), 2011. https://doi.org/10.3390/SU14042011

Nagai, Hiroko, Nakazawa, E., & Akabayashi, A. (2022). The creation of the Belmont Report and its effect on ethical principles. *Monash Bioethics Review*, *40*(2), 157–172. https://doi.org/10.1007/s40592-022-00165-5

Nagai, Hiroyuki, Nakazawa, E., & Akabayashi, A. (2022). The creation of the Belmont Report and its effect on ethical principles: a historical study. *Monash Bioethics Review*, *40*(2), 157. https://doi.org/10.1007/S40592-022-00165-5

Narayanan, A., & Shmatikov, V. (2006). *How To Break Anonymity of the Netflix Prize Dataset*. https://arxiv.org/abs/cs/0610105v2

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. *Proceedings - IEEE Symposium on Security and Privacy*, 111–125. https://doi.org/10.1109/SP.2008.33

Natural Sciences and Engineering Research Council of Canada. (2026). *NSERC - Natural Sciences and Engineering Research Council of Canada*. https://www.nserc-crsng.gc.ca/index_eng.asp

Neves, B. B., Amaro, F., & Fonseca, J. R. S. (2013). Coming of (Old) Age in the Digital Age: ICT Usage and Non-Usage among Older Adults. *Sociological Research Online*, *18*(2), 22–35. https://doi.org/10.5153/SRO.2998

Nielsen, O. B. (2017). A Comprehensive Review of Data Governance Literature. *Selected Papers of the IRIS, Issue Nr 8 (2017)*. https://aisel.aisnet.org/iris2017/3

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science (New York, N.Y.)*, *366*(6464), 447–453. https://doi.org/10.1126/SCIENCE.AAX2342

Office for Human Research Protections. (2026). *Office for Human Research Protections | HHS.gov*. https://www.hhs.gov/ohrp/index.html

Office of Privacy Commissioner of Canada, T. (2018). *Summary of privacy laws in Canada*. Summary of Privacy Laws in Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-3-1

*Office of the Privacy Commissioner of Canada*. (2015). 3 Years Ago. http://www.privacysense.net/10-privacy-principles-of-pipeda-accountability/

Office of the Privacy Commissioner of Canada. (2019). *PIPEDA fair information principles*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Oldevik, J., & Berre, A. J. (1998). UML-Based methodology for distributed systems. *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, 2–13. https://doi.org/10.1109/EDOC.1998.723237

Omran, Y., Henke, M., Heines, R., & Hofmann, E. (2009). Blockchain-driven supply chain finance: Towards a conceptual framework from a buyer perspective Yaghoob Omran. *Ipsera 2017*.

O'Neill, O. (2003). Some limits of informed consent. *Journal of Medical Ethics*, *29*(1), 4–7. https://doi.org/10.1136/JME.29.1.4

Ontañón M. (2020). *Progressive Disclosure - NN/G*. https://www.nngroup.com/articles/progressive-disclosure/

P. Galway, L., W. Parkes, M., Allen, D., & K. Takaro, T. (2016). Building Interdisciplinary Research Capacity: a Key Challenge for Ecological Approaches in Public Health. *AIMS Public Health*, *3*(2), 389–406. https://doi.org/10.3934/publichealth.2016.2.389

Panian, Z. (2010). Some Practical Experiences in Data Governance. *Undefined*.

Pedro, P. A., & Morita, P. P. (2022). A Proposed Personal Data Sovereignty Inter-Organizational Governance Framework for Public Health Research. *Proceedings - 2022 IEEE International Conference on Big Data, Big Data 2022*. https://doi.org/10.1109/BIGDATA55660.2022.10020348

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics 2018 137:8*, *137*(8), 575–582. https://doi.org/10.1007/S00439-018-1919-7

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/CYBSEC/TYY001

Poole, R., Gnann, A., & Hahn-Powell, G. (2019). Epistemic stance and the construction of knowledge in science writing: A diachronic corpus study. *Journal of English for Academic Purposes*, *42*, 100784. https://doi.org/10.1016/J.JEAP.2019.100784

Prictor, M., Lewis, M. A., Newson, A. J., Haas, M., Baba, S., Kim, H., Kokado, M., Minari, J., Molnár-Gábor, F., Yamamoto, B., Kaye, J., & Teare, H. J. A. (2020). Dynamic Consent: An Evaluation and Reporting Framework. *Journal of Empirical Research on Human Research Ethics*, *15*(3), 175–186. https://doi.org/10.1177/1556264619887073/ASSET/IMAGES/LARGE/10.1177_1556264619887073-FIG1.JPEG

Prinsen, L. (2024). Introducing dynamic consent for improved trust and privacy in research involving human biological material and associated data in South Africa. *Frontiers in Genetics*, *15*, 1272924. https://doi.org/10.3389/FGENE.2024.1272924

Prukalpa. (2021). *Data Governance Has a Serious Branding Problem*. https://towardsdatascience.com/data-governance-has-a-serious-branding-problem-7925b909712b

Rahimi, B., Safdari, R., & Jebraeily, M. (2014). Development of hospital information systems: User participation and factors affecting it. *Acta Informatica Medica*, *22*(6), 398–401. https://doi.org/10.5455/AIM.2014.22.398-401

Randazzo, S., & Sommerville, H. (2021). *The Theranos Revelations We Have Learned After 12 Weeks of the Elizabeth Holmes Trial - WSJ*. https://www.wsj.com/tech/what-elizabeth-holmes-theranos-trial-reveals-11631883936

Reichheld, F. (2006). Ultimate Question: For Driving Good Profits and True Growth (Hardcover). In *Harvard Business School Press Books*. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=19778403&site=bsi-live%5Cnhttp://harvardbusinessonline.hbsp.harvard.edu/relay.jhtml?name=itemdetail&id=7839

Resnik, D. B. (2009). Re-consenting human subjects: Ethical, legal and practical issues. In *Journal of Medical Ethics* (Vol. 35, Number 11, pp. 656–657). NIH Public Access. https://doi.org/10.1136/jme.2009.030338

Riordan, F., Papoutsi, C., Reed, J. E., Marston, C., Bell, D., & Majeed, A. (2015). Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK. *International Journal of Medical Informatics*, *84*(4), 237–247. https://doi.org/10.1016/j.ijmedinf.2015.01.008

Rivera, R., Borasky, D., Rice, R., Carayon, F., & Wong, E. (2007). Informed consent: An international researchers' perspective. In *American Journal of Public Health* (Vol. 97, Number 1, pp. 25–30). American Public Health Association. https://doi.org/10.2105/AJPH.2005.081604

Robinson Meyer. (2014). *Everything We Know About Facebook's Secret Mood Manipulation Experiment - The Atlantic*. The Atlantic. https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

Roseano, P., González, M., Borràs-Comes, J., & Prieto, P. (2016). Communicating Epistemic Stance: How Speech and Gesture Patterns Reflect Epistemicity and Evidentiality. *Discourse Processes*, *53*(3), 135–174. https://doi.org/10.1080/0163853X.2014.969137

Rosenbaum, S. (2010). Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access. *Health Services Research*, *45*(5p2), 1442–1455. https://doi.org/10.1111/j.1475-6773.2010.01140.x

Roski, J., Bo-Linn, G. W., & Andrews, T. A. (2017). Creating Value In Health Care Through Big Data: Opportunities And Policy Implications. *Https://Doi.Org/10.1377/Hlthaff.2014.0147*, *33*(7), 1115–1122. https://doi.org/10.1377/HLTHAFF.2014.0147

Rossi, A., & Palmirani, M. (2017). A visualization approach for adaptive consent in the European data protection framework. *Proceedings of the 7th International Conference for E-Democracy and Open Government, CeDEM 2017*, 159–170. https://doi.org/10.1109/CeDEM.2017.23

Rothwell, E., Brassil, D., Barton-Baxter, M., Brownley, K. A., Dickert, N. W., Ford, D. E., Kraft, S. A., McCormick, J. B., & Wilfond, B. S. (2021). Informed consent: Old and new challenges in the context of the COVID-19 pandemic. *Journal of Clinical and Translational Science*, *5*(1). https://doi.org/10.1017/CTS.2021.401

Safdari, R., Dargahi, H., Shahmoradi, L., & Farzaneh Nejad, A. (2012). Comparing four softwares based on ISO 9241 part 10. *Journal of Medical Systems*, *36*(5), 2787–2793. https://doi.org/10.1007/S10916-011-9755-5

Saksono, H., & Parker, A. G. (2024). Socio-Cognitive Framework for Personal Informatics: A Preliminary Framework for Socially-Enabled Health Technologies. *ACM Transactions on Computer-Human Interaction*, *31*(3). https://doi.org/10.1145/3674504/ASSET/6448212F-6482-4F37-96EB-F44C81B0CDEE/ASSETS/IMAGES/LARGE/TOCHI-2022-0275-F10.JPG

Schröder-Bäck, P., Duncan, P., Sherlaw, W., Brall, C., & Czabanowska, K. (2014). Teaching seven principles for public health ethics: towards a curriculum for a short course on ethics in public health programmes. *BMC Medical Ethics*, *15*(1). https://doi.org/10.1186/1472-6939-15-73

Schunk, D. H., & DiBenedetto, M. K. (2020). Motivation and social cognitive theory. *Contemporary Educational Psychology*, *60*, 101832. https://doi.org/10.1016/J.CEDPSYCH.2019.101832

Scott, A. S., Goldsmith, M., Teare, H., Creese, S., & Kaye, J. (2018). *Dynamic Consent in Cybersecurity for Health*.

Selic, B. (1998). Using UML for modeling complex real-time systems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1474*, 250–260. https://doi.org/10.1007/BFb0057795

Sheehan, M., Thompson, R., Fistein, J., Davies, J., Dunn, M., Parker, M., Savulescu, J., & Woods, K. (2019). Authority and the Future of Consent in Population-Level Biomedical Research. *Public Health Ethics*, *12*(3), 225–236. https://doi.org/10.1093/PHE/PHZ015

Simons, C., & Wirtz, G. (2007). Modeling context in mobile distributed systems with the UML. *Journal of Visual Languages and Computing*, *18*(4), 420–439. https://doi.org/10.1016/j.jvlc.2007.07.001

Sims, J. M. (2010). A brief review of the Belmont report. *Dimensions of Critical Care Nursing*, *29*(4), 173–174. https://doi.org/10.1097/DCC.0b013e3181de9ec5

Six, N., Herbaut, N., & Salinesi, C. (2022). Blockchain software patterns for the design of decentralized applications: A systematic literature review. *Blockchain: Research and Applications*, *3*(2), 100061. https://doi.org/10.1016/J.BCRA.2022.100061

Smith, C. M. (2005). Origin and uses of primum non nocere--above all, do no harm! *Journal of Clinical Pharmacology*, *45*(4), 371–377. https://doi.org/10.1177/0091270004273680

Social Sciences and Humanities Research Council of Canada. (2026). *Social Sciences and Humanities Research Council*. https://sshrc-crsh.canada.ca/en.aspx

Spencer, K., Sanders, C., Whitley, E. A., Lund, D., Kaye, J., & Dixon, W. G. (2016). Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: A qualitative study. In *Journal of Medical Internet Research* (Vol. 18, Number 4, p. e66). JMIR Publications Inc. https://doi.org/10.2196/jmir.5011

Steelman, K. S., Tislar, K. L., Ureel, L. C., & Wallace, C. (2016). Breaking Digital Barriers: A Social-Cognitive Approach to Improving Digital Literacy in Older Adults. *Communications in Computer and Information Science*, *617*, 445–450. https://doi.org/10.1007/978-3-319-40548-3_74

Stein, D. T., & Terry, S. F. (2013). Reforming Biobank Consent Policy: A Necessary Move Away from Broad Consent Toward Dynamic Consent. *Genetic Testing and Molecular Biomarkers*, *17*(12), 855–856. https://doi.org/10.1089/gtmb.2013.1550

Steinsbekk, K. S., & Solberg, B. (2011). Biobanks--When is Re-consent Necessary? *Public Health Ethics*, *4*(3), 236–250. https://doi.org/10.1093/phe/phr031

Strayer, C., & Grebliunas, R. (2024). *Indigenous Data Sovereignty and Governance*. BCcampus. https://opentextbc.ca/indigenousdigitalliteracies/chapter/indigenous-data-sovereignty/

Strzelecki, A. (2022). The Apple Mobility Trends Data in Human Mobility Patterns during Restrictions and Prediction of COVID-19: A Systematic Review and Meta-Analysis. *Healthcare*, *10*(12), 2425. https://doi.org/10.3390/HEALTHCARE10122425

Sugarman, J., Lavori, P. W., Boeger, M., Cain, C., Edson, R., Morrison, V., & Yeh, S. S. (2005). Evaluating the quality of informed consent. *Clinical Trials*, *2*(1), 34–41. https://doi.org/10.1191/1740774505cn066oa

Tang, M. (2023). The challenge of the cloud: between transnational capitalism and data sovereignty. *The Geopolitics of Chinese Internets*, 63–77. https://doi.org/10.4324/9781032690162-5/CHALLENGE-CLOUD-TRANSNATIONAL-CAPITALISM-DATA-SOVEREIGNTY-MIN-TANG

Tao, D., Shao, F., Wang, H., Yan, M., & Qu, X. (2020). Integrating usability and social cognitive theories with the technology acceptance model to understand young users' acceptance of a health information portal. *Health Informatics Journal*, *26*(2), 1347–1362. https://doi.org/10.1177/1460458219879337/ASSET/9087EE9B-3102-4828-868F-1E0B65C0E69E/ASSETS/IMAGES/LARGE/10.1177_1460458219879337-FIG2.JPG

Tarrant, D., Brody, T., & Carr, L. (2009). *From the Desktop to the Cloud: Leveraging Hybrid Storage Architectures in your Repository*.

Teare, H. J. A., Prictor, M., & Kaye, J. (2020). Reflections on dynamic consent in biomedical research: the story so far. *European Journal of Human Genetics 2020 29:4*, *29*(4), 649–656. https://doi.org/10.1038/s41431-020-00771-z

Technical Committee ISO/IEC JTC 1. (2022). *ISO/IEC 27701:2019 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. https://www.iso.org/standard/71670.html

Technical Committee ISO/TC 215. (2021). *ISO - ISO/DIS 23903 - Health informatics — Interoperability and Integration Reference Architecture – Model and Framework*. https://www.iso.org/standard/77337.html

Thomas, G. (2010). *The DGI Data Governance Framework*.

Thompson, R., & McNamee, M. J. (2017). Consent, ethics and genetic biobanks: the case of the Athlome project. *BMC Genomics*, *18*(S8), 830. https://doi.org/10.1186/s12864-017-4189-1

Thorogood, A., Simkevitz, H., Phillips, M., Dove, E. S., & Joly, Y. (2017). Protecting the Privacy of Canadians' Health Information in the Cloud. *Canadian Journal of Law and Technology*, *14*(1).

Tiwana, A., Konsynski, B., & Venkatraman, N. (2013). Special issue: Information technology and organizational governance: The IT governance cube. *Journal of Management Information Systems*, *30*(3), 7–12. https://doi.org/10.2753/MIS0742-1222300301

Tong, H. L., Coiera, E., & Laranjo, L. (2018). Using a Mobile Social Networking App to Promote Physical Activity: A Qualitative Study of Users' Perspectives. *J Med Internet Res 2018;20(12):E11439 Https://Www.Jmir.Org/2018/12/E11439*, *20*(12), e11439. https://doi.org/10.2196/11439

Tovino, S. A. (2017). The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons. *Undefined*.

Troquard, N., & Balbiani, P. (2007). *Propositional Dynamic Logic*.

Tse, D., Chow, C., Ly, T., Tong, C., & Tam, K. (2018a). The Challenges of Big Data Governance in Healthcare. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing*

*And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1632–1636. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00240

Tse, D., Chow, C., Ly, T., Tong, C., & Tam, K. (2018b). The Challenges of Big Data Governance in Healthcare. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1632–1636. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00240

Turner, D. W. (2010). Qualitative Interview Design: A Practical Guide for Novice Investigators. *The Qualitative Report*, *15*(3), 754–760. https://doi.org/10.46743/2160-3715/2010.1178

Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., Pathan, M. S., & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon*, *10*(16), e34407. https://doi.org/10.1016/J.HELIYON.2024.E34407

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581

U.S Food & Drug Administration. (2018). *Informed Consent for Clinical Trials*. https://www.fda.gov/forpatients/clinicaltrials/informedconsent/default.htm#What_is_Informed_Consent_

U.S. Food and Drug Administration. (2026a). *eCFR :: 21 CFR 21.72 -- Individual consent to disclosure of records to other persons.* https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-21/subpart-G/section-21.72

U.S. Food and Drug Administration. (2026b). *eCFR :: 21 CFR Part 11 - Electronic Records; Electronic Signatures*. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11

U.S. Food and Drug Administration. (2026c). *eCFR :: 21 CFR Part 50 Subpart B -- Informed Consent of Human Subjects*. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-50/subpart-B

U.S. Food and Drug Administration. (2026d). *eCFR :: 45 CFR 164.502 -- Uses and disclosures of protected health information: General rules.* https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.502?utm_source=chatgpt.com

U.S. Food and Drug Administration. (2026e). *eCFR :: 50 CFR Part 37 Subpart F -- Reporting and Data Management*. https://www.ecfr.gov/current/title-50/chapter-I/subchapter-C/part-37/subpart-F

U.S. Food and Drug Administration. (2026f). *U.S. Food and Drug Administration*. https://www.fda.gov/

U.S. Food and Drug Administration. (2026g). *Use of Electronic Informed Consent in Clinical Investigations – Questions and Answers | FDA*. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/use-electronic-informed-consent-clinical-investigations-questions-and-answers

van Deursen, A. J. A. M., Helsper, E. J., & Eynon, R. (2015). Development and validation of the Internet Skills Scale (ISS). *Https://Doi.Org/10.1080/1369118X.2015.1078834*, *19*(6), 804–823. https://doi.org/10.1080/1369118X.2015.1078834

van Deursen, A. J. A. M., Helsper, E. J., & Eynon, R. (2016). Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society*, *19*(6), 804–823. https://doi.org/10.1080/1369118X.2015.1078834

Van Panhuis, W. G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A. J., Heymann, D., & Burke, D. S. (2014). A systematic review of barriers to data sharing in public health. *BMC Public Health*, *14*(1), 1–9. https://doi.org/10.1186/1471-2458-14-1144/TABLES/1

Velmovitsky, P. E., Souza Miranda, P. A. D. S. E., Vaillancourt, H., Donovska, T., Teague, J., & Morita, P. P. (2020). A Blockchain-Based Consent Platform for Active Assisted Living: Modeling Study and Conceptual Framework. *J Med Internet Res 2020;22(12):E20832 Https://Www.Jmir.Org/2020/12/E20832*, *22*(12), e20832. https://doi.org/10.2196/20832

Wallace, S. E., & Miola, J. (2021). Adding dynamic consent to a longitudinal cohort study: A qualitative study of EXCEED participant perspectives. *BMC Medical Ethics*, *22*(1). https://doi.org/10.1186/S12910-021-00583-W

Walport, M., & Brest, P. (2011). Sharing research data to improve public health. *Lancet*, *377*(9765), 537–539. https://doi.org/10.1016/s0140-6736(10)62234-9

Wang, C. J., Ng, C. Y., & Brook, R. H. (2020). Response to COVID-19 in Taiwan. *JAMA*, *323*(14), 1341. https://doi.org/10.1001/jama.2020.3151

Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D., & Jing, J. (2020). Blockchain-based Certificate Transparency and Revocation Transparency. *IEEE Transactions on Dependable and Secure Computing*, 1–1. https://doi.org/10.1109/tdsc.2020.2983022

Welzel, C., Ostermann, M., Smith, H. L., Minssen, T., Kirsten, T., & Gilbert, S. (2025). Enabling secure and self determined health data sharing and consent management. *NPJ Digital Medicine*, *8*(1), 560. https://doi.org/10.1038/S41746-025-01945-Z

Wende, K. (2007). A Model for Data Governance – Organising Accountabilities for Data Quality Management. *ACIS 2007 Proceedings*. https://aisel.aisnet.org/acis2007/80

Wendl, M., Doan, M. H., & Sassen, R. (2023). The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *Journal of Environmental Management*, *326*, 116530. https://doi.org/10.1016/J.JENVMAN.2022.116530

Will, T. (2026). *PSSUQ (Post-Study System Usability Questionnaire) - UIUX Trend*. https://uiuxtrend.com/pssuq-post-study-system-usability-questionnaire/

Williams, H., Spencer, K., Sanders, C., Lund, D., Whitley, E. A., Kaye, J., & Dixon, W. G. (2015). Dynamic Consent: A Possible Solution to Improve Patient Confidence and Trust in How Electronic Patient Records Are Used in Medical Research. *JMIR Med Inform 2015;3(1):E3 Https://Medinform.Jmir.Org/2015/1/E3*, *3*(1), e3525. https://doi.org/10.2196/MEDINFORM.3525

Winter, J. S., & Davidson, E. (2019a). Big data governance of personal health information and challenges to contextual integrity. *Information Society*, *35*(1), 36–51. https://doi.org/10.1080/01972243.2018.1542648

Winter, J. S., & Davidson, E. (2019b). Governance of artificial intelligence and personal health information. *Digital Policy, Regulation and Governance* , *21*(3), 280–290. https://doi.org/10.1108/DPRG-08-2018-0048/FULL/XML

Wu, D., Verhulst, S. G., Pentland, A., Avila, T., Finch, K., & Gupta, A. (2021). How data governance technologies can democratize data sharing for community well-being. *Data & Policy*, *3*. https://doi.org/10.1017/DAP.2021.13

Xie, P., Yan, W., Xuan, P., Zhu, J., Wu, Y., Li, X., & Zou, J. (2018, December 19). Conceptual Framework of Blockchain-based Electricity Trading for Neighborhood Renewable Energy. *2nd IEEE Conference on Energy Internet and Energy System Integration, EI2 2018 - Proceedings*. https://doi.org/10.1109/EI2.2018.8581887

Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). *Applying Software Patterns to Address Interoperability in Blockchain-based Healthcare Apps*. http://arxiv.org/abs/1706.03700

Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. *Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*, 268–275. https://doi.org/10.1109/CLOUD.2010.62

Zhang, W., Zhao, H., & Mei, H. (2004). A Propositional Logic-Based Method for Verification of Feature Models. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3308*, 115–130. https://doi.org/10.1007/978-3-540-30482-1_16

Zheng, X., Mukkamala, R. R., Vatrapu, R., & Ordieres-Mere, J. (2018, November 9). Blockchain-based personal health data sharing system using cloud storage. *2018 IEEE 20th International Conference*

*on E-Health Networking, Applications and Services, Healthcom 2018*. https://doi.org/10.1109/HealthCom.2018.8531125

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017a). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017b). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017. https://doi.org/10.1109/BigDataCongress.2017.85

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 180–184. https://doi.org/10.1109/SPW.2015.27

# Appendix A

## 14. Hyperledger Fabric Details

In Hyperledger Fabric, Organizations can communicate with each other on an HFN by creating and using communication channels. Communication channels are private communication environments for all or a subset of the organization's members of a consortium. New organizations are enrolled in the HFN through a trusted Membership Service Provider (*Membership Service Provider (MSP) — Hyperledger-Fabricdocs Master Documentation*, n.d.), which is responsible for issuing and validating certificates, and user authentication.

The conduction of business transactions between organizations of an HFN consortium is stored in a ledger. A ledger stores both the current state and history of states from a business object. To keep a business object, the current state HF uses a database called world-state (*Membership — Hyperledger-Fabricdocs Master Documentation*, n.d.), which will be explained later in this paper. To store the history of the transactions of a business object, HF utilizes a blockchain data structure (Androulaki et al., 2018b). Together, the blockchain structure and world-state, are what allow the ledger to hold an immutable history of business objects' states (blockchain) and provide fast access to the most recent state of a single business object.

Participants of the HFN achieve consensus by following a transaction flow that takes into account the endorsement policy assigned to smartcontracts (*Chaincode for Developers — Hyperledger-Fabricdocs Master Documentation*, n.d.). This means that transactions can only be accepted into the ledger if all, or a subset of, the endorsing peers of a consortium approve the transaction. Smart contracts in HFN are a software representation of a contract that governs the processes that alter the state of a business object. In Hyperledger Fabric smartcontracts are packaged into a structure called chaincode, which consists of multiple smartcontracts. Each chaincode is deployed into an HFN channel with an endorsement policy assigned to it. The endorsement represents which organizations must sign a transaction, so it is accepted and added to the ledger.

This transaction flow from HF relies on identity validation for members of the network. All transactions are sent to the network first as a proposal that needs to be endorsed by all HFN organizations included in the smart-contract's policy. The proposal is signed using user's cryptographic credentials that generate a unique signature for the proposal.

Endorsement organizations from HFN verify transactions for (i) A well-formed transaction proposal; (ii) It is not a repeated proposal; (iii) Checks with the Membership Service Provider (MSP) (*Membership Service Provider (MSP) — Hyperledger-Fabricdocs Master Documentation*, n.d.) to verify that the proposal signature is correct. (iv) Uses MSP to verify the proposal submitter identity has the authorization to perform operations in that channel.

Input parameters are fed to the chaincode that is going to be executed against the current world-state. After the peer finishes executing the chaincode, it returns the result alongside with the peer signature to the client as a proposal response. Finally, the client inspects the response from peers, and if all the necessary signatures are valid, the transaction is created.

The client application broadcasts the transaction to the ordering service that, in turn, orderly creates blocks of transactions and sends them to the channel's peers. Each peer verifies the block transactions and signatures before adding the block to the ledger. Hyperledger Fabric is not the only appropriate platform that can provide the necessary infrastructure to instantiate our conceptual framework. For example, Ethereum (Buterin, 2013) is a blockchain solution that gives full support for distributed applications over a blockchain network. Even if Ethereum's main network is public, which is not ideal for the healthcare domain, it can be instantiated into a private network environment, thus becoming compliant with the privacy and access control requirements of the present conceptual framework. We refer to Modum.io (Bocek et al., 2017), as an example of an implementation of a supply-chain management system applied to Ethereum. Modum.io enables pharmaceutics companies to monitor the temperature and humidity of medical products by using smart contracts to verify sensor data during its life cycle.

Other honourable mentions of blockchain platforms that are appropriate to this framework instantiation are the IBM blockchain Platform (IBM, 2020), the Multichain Private blockchain (Greenspan, 2015), the Hydra chain (*Hydrachain/Hc_consensus_explained.Md at Develop · HydraChain/Hydrachain · GitHub*, n.d.), and the BigchainDB (Mcconaghy et al., 2016). It is also worth mentioning that using these technologies will require some changes in the framework's Hyperledger Fabric Network (HFN) (Hyperledger, 2019a) component.

The table below contains the platform minimum requirements mapped over HF's attributes, providing a checklist to develop the platform.

*Table 26 - Dynamic Consent Management Platform Requirements.*

| *Solution Requirements* | *Hyperledger Fabric* |
|---|---|
| *Privacy of patient's information* | HF uses cryptographic material to control access to the ledger. Applications from authorized organizations keep information from patients in their infrastructure. HF only stores anonymized consent information from unique keys created for each patient. |
| *Private communications between stakeholders of the informed consent process* | HF maps stakeholders from a network into organizations. Each organization can be a part of a channel composed of some other organizations that constitute the consortium. Communications inside a channel are private to their members. |
| *Scalable and fast querying of the ledger* | HF stores the most recent state of a business object in a state database called world-state. Every time an informed consent state changes or a new informed consent is created, a new transaction is inserted into the ledger. But the world-state only updates the business object if he already exists, otherwise, it is created. These characteristics also make HF more scalable since querying the ledger's complete history is not required for knowing the most recent informed consent status. |
| *No cryptocurrency* | HF has no cryptocurrency, which complies with our 'solution's intention to provide the simplest solution possible to our end users, which are people using AAL. |
| *Security of information* | Since HF is a private and permissioned blockchain platform, the security of information is much less susceptible to a privacy breach. |
| *Immutability of ledger history* | HF provides an immutable ledger natively. |
| *Accountability of informed consent transactions* | With HF, smart contracts can be created enforcing standards. These smart contracts can be configured to explicitly require the endorsement of an organization that represents an auditing authority. |
| *SDK for development of end-user Applications capable of interacting with the ledger* | In order for our conceptual framework to be instantiated, the creation of web applications capable of interacting with the blockchain network to create and retrieve consent transactions is necessary. HF provides such SDKs in NodeJS, Java, and Go languages. |
| *Smart-contracts capabilities* | Smart contracts are needed to ensure the enforcement of standards and endorsements that must be respected so that a new informed consent transaction is accepted and stored in the ledger. |
| *Custom network policies* | Such policies are needed to control network interactions between organizations. The informed consent process has its own unique policing needs, such as endorsement policies, hence the need for customization. |
| *Extensibility of the network* | For our solution's relevancy, the capability of adding new organizations, policies, channels, and smart contracts without having to start a new network is imperative. HF provides the plug-and-play capability for adding new entities into an existing network. |

# Appendix B

## 15. Use-case Diagram Descriptions

Each use case is presented with a concise goal statement, actors, triggering conditions, main and alternate flows, exception handling, and the attached governance obligations expressed as UI guards, validators, and audit hooks. Where relevant, obligations reference formal invariants (e.g., dual approval before start), Dynamic Consent rules, and Consent Privacy Impact Quantification (CPIQ) (Appenzeller et al., 2021) thresholds, aligning operational behaviour with the compliance expectations of TCPS2/GDPR and institutional policy (Canadian Institutes of Health Research, 2022; European Parliament and of the Council of 27 April 2016, 2016; Office of the Privacy Commissioner of Canada, 2019). Acceptance criteria and measurable indicators—such as blocked-action rates by rule, consent/re-consent latency, and withdrawal integrity—connect these obligations to the evaluation scaffolding introduced earlier, ensuring that trust, usability, and accountability are assessed against clearly defined, verifiable requirements.

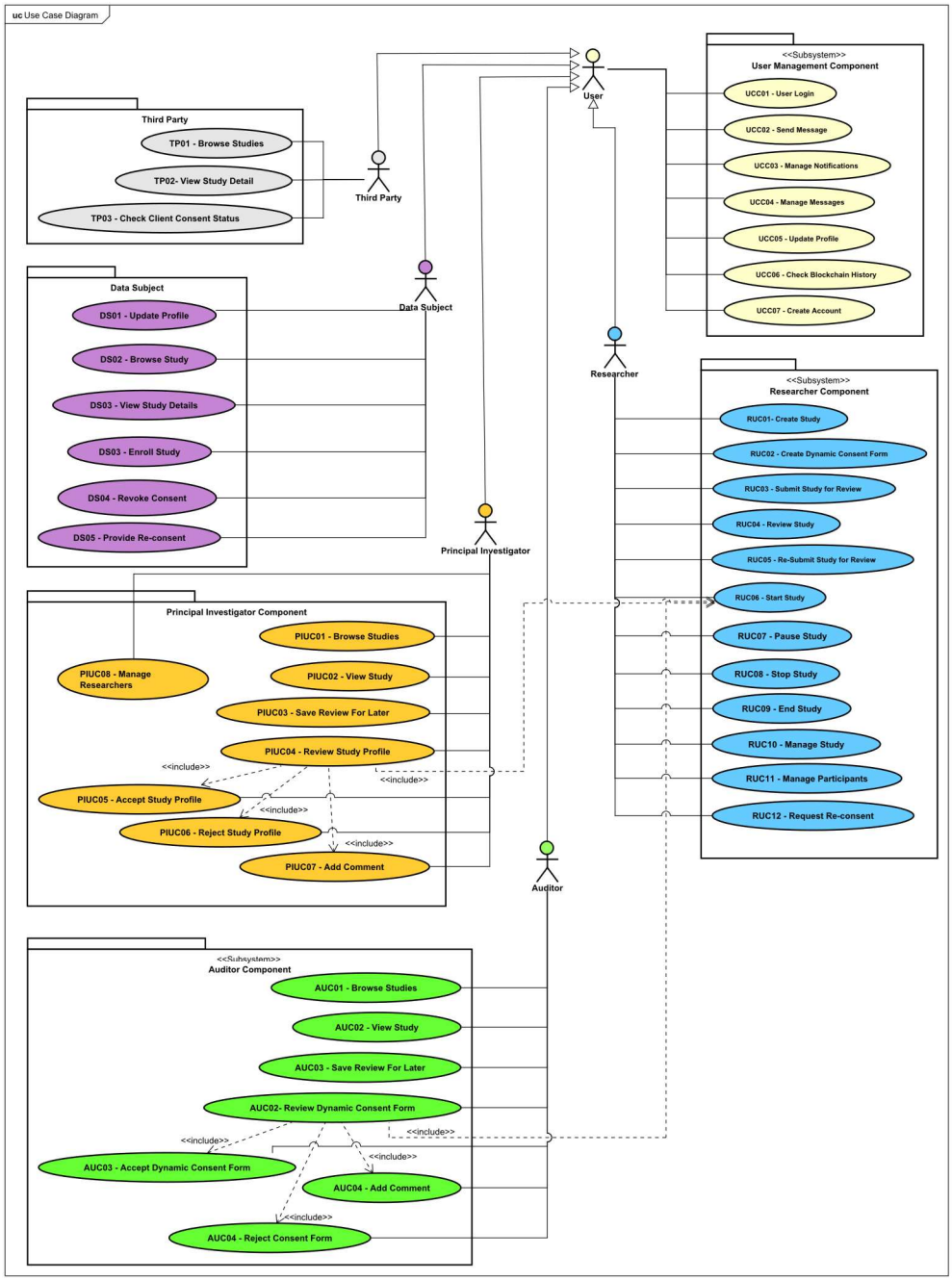



*Figure 17 - Use case diagram of platform users.*

Each use-case specification includes pre- and postconditions that precisely capture the governance rules (e.g., endorsement policies, minimum quorum, and revocation-propagation time ≤ 1s). By baking regulatory text into class-level invariants, we prevent divergence between the legal model and the executable system.

## 15.1. Handling Cross-Cutting Concerns

The diagram highlights two <<include>> relationships—Authenticate User and Log Action—which are invoked by every critical use case. They operationalize the framework's relational mechanisms:

- Authenticate User enforces role-based access controls derived from governance role definitions.
- Log Action routes a signed transaction to Hyperledger Fabric for indelible storage, satisfying the auditability requirement.

## 15.2. Implications for Implementation

The UML model is not merely descriptive: it drives the micro-service boundaries (each top-level use case is served by an independent NodeJS service), the Fabric channel design (participant-facing actions vs. custodial queries), and the automated test harness (Cucumber scenarios are generated directly from use-case success paths). Consequently, updates to the governance framework can be propagated through the same model, guaranteeing consistent evolution of policy and code.

In summary, the UML use-case diagram provides a governance-centered blueprint of Consentio. It demonstrates conformance of system behaviour to the roles, rules and accountability relationships articulated in Chapter 1, and establishes a verifiable contract that Chapter 3 usability and compliance testing can measure against.

## 15.3. Comprehensive Catalogue of All Use-Cases

The tables below present the description of all use-cases mapped for the solution based in the data governance requirements and the requirements of web-based management systems that is generally applied, such as user-based authentication.

*Table 27 - Catalogue of all use-cases that appear in Section 7 UML diagram.*

| # | Use-Case Label | Purpose & Governance Link |
|---|---|---|
| | | **Generic User Component** |
| **1** | UUC01 USER LOGIN | Platform gatekeeper; enforces identity, authentication & auditability required by the governance framework. |
| **2** | UUC02 SEND MESSAGE | Secure channel that realises the Negotiation / Reciprocity transactions between actors (GAF). |
| **3** | UUC03 MANAGE NOTIFICATIONS | Les any actor control notification flow generated by smart contracts (e.g., consent revocation). |
| **4** | UUC04 MANAGE MESSAGES | CRUD operations on messages; fulfils transparency & accountability principles in governance. |
| **5** | UUC05 UPDATE PROFILE | Keeps actor metadata current for accurate role-based-access and delegated authority. |
| **6** | UUC06 CHECK BLOCKCHAIN HISTORY | Human-readable front-end to the ledger; enables auditability of every Dynamic Consent (DIC) transaction. |
| **7** | UUC07 CREATE ACCOUNT | On-boards actors under PI or third-party governance rules (PIUC08 / TP01); initializes identity mapping. |
| | | **Public Health Researcher Component** |
| **8** | RUC01 CREATE STUDY | Instantiates a study shell; binds researcher identity to governance obligations and lifecycle duties. |
| **9** | RUC02 CREATE DYNAMIC CONSENT FORM | Crafts DIC template under data sovereignty, privacy, and IRB guidance; foundational compliance artifact. |
| **10** | RUC03 SUBMIT STUDY FOR REVIEW | Sends the study profile to PI (PIUC04); a Directive transaction representing internal governance workflow. |
| **11** | RUC04 REVIEW STUDY | Enables self-audit before submission; improves efficiency and reduces governance loop friction. |
| **12** | RUC05 RE-SUBMIT STUDY FOR REVIEW | Iterative improvement after supervisory (PI) comments; ensures completeness before IRB submission. |
| **13** | RUC06 START STUDY | Triggers participant recruitment; initializes consent acquisition (DS04). |
| **14** | RUC07 PAUSE STUDY | Temporarily suspends enrollment while preserving prior consent state on the ledger. |
| **15** | RUC08 STOP STUDY | Terminates protocol participation but retains audit trail; locks future edits. |
| **16** | RUC09 END STUDY | Archives the study and sends outputs to custodians; fulfills governance end-of-life obligations. |
| **17** | RUC10 MANAGE STUDY | Maintains and edits study metadata; reflects “data lifecycle” control node in governance mapping. |
| **18** | RUC11 MANAGE PARTICIPANTS | Interfaces with subject cohort; supports actor-to-actor reciprocity under personal data governance. |
| **19** | RUC12 REQUEST RE-CONSENT | Issues updated DIC version after protocol changes; enables compliance continuity and traceability. |
| | | **Principal Investigator Component** |
| **20** | PIUC01 BROWSE STUDIES | Overview dashboard; supports role as supervisory actor under ISO/IEC 38500. |
| **21** | PIUC02 VIEW STUDY | Allows metadata and protocol inspection at individual study level; supports granular oversight. |
| **22** | PIUC03 SAVE REVIEW FOR LATER | Enables staged reviews; fulfills Evaluate principle of organizational governance. |

| | | |
|---|---|---|
| **23** | PIUC04 REVIEW STUDY PROFILE | Checks researcher submission against policy and regulatory frameworks. |
| **24** | PIUC05 ACCEPT STUDY PROFILE | Grants PI-level approval; emits a smart contract event committing the decision to the ledger. |
| **25** | PIUC06 REJECT STUDY PROFILE | Ensures only compliant studies proceed; enforces critical gatekeeping in governance hierarchy. |
| **26** | PIUC07 ADD COMMENT | Provides structured, auditable feedback; enhances transparency in directive transactions. |
| **27** | PIUC08 MANAGE RESEARCHERS | Assigns researcher roles; governs role-based access, responsibility, and accountability boundaries. |
| | **Auditor & Institutional Review Board Component** | |
| **28** | AUC01 BROWSE STUDIES | Lists protocols needing ethical review; supports workload management and IRB prioritization. |
| **29** | AUC02 VIEW STUDY | Opens a detailed dossier for ethical assessment and privacy compliance verification. |
| **30** | AUC03 SAVE REVIEW FOR LATER | Drafts ethics decision; supports non-linear workflows in IRB governance. |
| **31** | AUC04 REVIEW DYNAMIC CONSENT FORM | Formal compliance review of DIC format, language, scope, and participant protections. |
| **32** | AUC05 ADD COMMENT | Enables revision instructions; documents required changes for downstream actors. |
| **33** | AUC06 ACCEPT DYNAMIC CONSENT FORM | Final ethics approval; commits IRB signature hash to the ledger. |
| **34** | AUC07 REJECT CONSENT FORM | Prevents flawed protocols from deploying; critical directive transaction in consent governance. |
| | **Data Subject Component** | |
| **35** | DS01 UPDATE PROFILE | Updates personal metadata used to scope consent terms (e.g., region, contact, wearable IDs). |
| **36** | DS02 BROWSE STUDY | Supports autonomy through study discovery; reflects voluntary nature of participation. |
| **37** | DS03 VIEW STUDY DETAILS | Ensures full risk-benefit disclosure before enrollment decision; fulfills informed consent. |
| **38** | DS04 ENROLL STUDY | Executes DIC smart contract; adds immutable consent record. |
| **39** | DS05 REVOKE CONSENT | Invokes withdrawal rights under GDPR/TCPS2; triggers revocation events and data flow termination. |
| **40** | DS06 PROVIDE RE-CONSENT | Responds to protocol amendments; logs new DIC version and timestamped consent event. |
| | **Third-party component (data custodian and data provider)** | |
| **41** | TP01 BROWSE STUDIES | Displays studies that have accessed or requested client PHI; supports custodial visibility. |
| **42** | TP02 VIEW STUDY DETAIL | Enables examination of scope and duration of authorized data use before processing. |
| **43** | TP03 CHECK CLIENT CONSENT STATUS | Validates live consent status using blockchain ledger; ensures compliant data exchange. |

## 15.4. How the Diagram Mirrors Chapter 1's Data Governance Framework

The governance diagram effectively reflects the Chapter 1 governance framework by aligning each actor identified—Researcher, Principal Investigator, Auditor/Institutional Review Board (IRB), Data Subject, and Third Party—directly with the respective stakeholder groups outlined in the Governance Analytical Framework (GAF). This alignment ensures consistency in actor roles and responsibilities and provides clarity in stakeholder engagement throughout the research lifecycle. By mapping these actors distinctly, the diagram facilitates explicit identification and engagement of stakeholders in the governance process, thereby promoting transparency and accountability in research governance.

Moreover, the operationalization of governance principles through various transaction types—negotiation, directive, distribution, and reciprocities are clearly demonstrated. Negotiation and reciprocity transactions are specifically implemented through functionalities such as messaging and notifications (UCC02-UCC04, PIUC07, AUC05), promoting ongoing dialogue and consensus-building among stakeholders. Directive transactions, where approval or rejection of artifacts generated by another party is mandated, are operationalized through paired use cases like RUC03 linking to PIUC05/06 and RUC02 linking to AUC06/07, clearly illustrating authority relationships within the governance structure.

Distribution of knowledge and value is achieved through practical tools for ledger-history inspection (UCC06) and functionalities related to study export and closure (RUC09, RUC10), enhancing transparency and facilitating auditability. Additionally, the framework's foundational principle of data sovereignty is meticulously implemented, providing data subjects with fine-grained, reversible controls over Personal Health Information (PHI) via specific functionalities (DS01-DS06), thus operationalizing personal data sovereignty principles that underpin the overall governance model.

## 15.5. Governance Loops and Compliance with International Standards

The governance loops identified in Chapter 1 are comprehensively represented through structured processes for iterative review and commentary, exemplified by the use cases PIUC03-07 and AUC03-05. These processes explicitly embody the Evaluate–Direct–Monitor governance cycle as recommended by ISO/IEC

38500 (Calder, 2019). Such iterative mechanisms are critical to maintaining ongoing evaluation, clear directive communication, and continuous monitoring within the governance framework. They facilitate continuous improvement, allowing stakeholders to refine study profiles and consent forms, ensuring compliance and adaptability to evolving ethical standards and research requirements.

The practical translation of theoretical governance structures into concrete platform functionalities underscores the diagram's role in bridging policy with actionable practice. Every defined stakeholder obligation and right are matched with an operational counterpart within the software architecture, providing stakeholders with tangible tools to fulfill their governance roles effectively. This explicit linkage ensures adherence to both ethical and legal standards, significantly enhancing stakeholder confidence in the governance mechanisms. Consequently, this design supports robust stakeholder engagement, encourages compliance, and reinforces the credibility of the governance processes employed in public health research.

Collectively, the use-cases translate the abstract governance structure of Chapter 1 into concrete, verifiable platform functionality, ensuring that every stakeholder obligation and right has an operational counterpart in the software architecture.

# Appendix C

## 16. Descriptions of the Platform Classes from the Class Diagram

This appendix summarizes all classes represented in the UML class diagram, grouped by aggregate, with brief statements of their key attributes and responsibilities, and how they correspond to the governance actors defined in Section 7. In the diagram notation, «interface» denotes a pure interface, ▷ denotes inheritance, ◆ denotes composition, and ◁ denotes aggregation.

### 16.1. Identity and Access Aggregate

The identity and access aggregate establishes authenticated participation, role assignment, and policy enforcement across the platform. The abstract root User provides the common identity surface, including identifiers and core credentials, such as ID, name, email, password hash, and role, and represents a generic stakeholder that becomes specialized through concrete subclasses. Address captures postal and provenance attributes used to represent contextual identity details relevant to data-subject provenance. Invitation supports controlled onboarding through a tokenized mechanism that includes an expiry time and an offered role, enabling auditable enrolment workflows. Rule encapsulates fine-grained governance policy logic through an identifier and an expression encoded as JSON-logic, operationalizing the policy constraints derived from the inter-organizational data governance duties. Parameter stores sensor and metric metadata required for consistent interpretation of incoming data streams and quality constraints. Notification formalizes transparency and alerting duties through sender, receiver, and message fields, supporting user-facing communication obligations that arise from governance requirements.

The **Role** enumeration defines the platform's governed identities and includes **Participant**, **Researcher**, **PrincipalInvestigator**, **Auditor**, **ThirdParty**, and **Admin**.

## 16.2. Research Lifecycle Aggregate

The research lifecycle aggregate represents the end-to-end study domain and the artefacts required to describe, publish, operate, and govern a study. Study is the central project artefact and includes identifiers and descriptive fields such as title and objective, as well as governance-relevant declarations such as data collected, data sharing, status, and timestamps. **StudyCategory** provides a controlled vocabulary that supports harmonization and standardization across studies. **StudyTraits** captures boolean and categorical flags used for risk and governance classification, for example whether data are anonymized and whether additional assets are involved. **StudyProfile** represents public-facing metadata, including principal investigator contact information, and operationalizes transparency by making study intent and oversight legible to participants. **StudyParticipantProfile** tracks per-participant progress and incentive accumulation, supporting monitoring obligations and participation management. **Reward** defines incentive governance through type and value. **Device** represents data-source provenance through make, model, and a trust score. **Record** points to PHI payload references rather than duplicating raw content, aligning with minimization and modular data handling practices. Finally, the Status enumeration captures study lifecycle states and includes Draft and Pending.

## 16.3. Interfaces for Command Segregation and Separation of Duty

The platform enforces separation of duty by expressing actor capabilities through role-specific action interfaces. **ResearcherAction** includes operations to create a study, submit it for review, start, stop, or pause it, create dynamic consent forms, and request reconsent. **PrincipalInvestigatorAction** supports oversight through accepting or rejecting study profiles and participating in threaded comments. **AuditorAction** governs ethical vetting by accepting or rejecting a dynamic consent form. **ThirdPartyAction** supports disclosure controls by validating participant consent, including retrieving consent by participant identifier and retrieving consent states for study participants. ParticipantAction expresses participant self-determination through saving a study, giving consent, revoking consent, providing reconsent, and retrieving dynamic consent history. Concrete subclasses, **Participant**,

**Researcher**, **PrincipalInvestigator**, **Auditor**, and **ThirdParty**, extend **User** and implement their respective interfaces, ensuring that authority is constrained to the governance-aligned responsibilities assigned to each actor.

## 16.4. Dynamic Consent and Ledger Aggregate

The dynamic consent and ledger aggregate operationalizes ethical transparency, accountability, and auditability, while supporting personal data sovereignty at the level of a subject–study relationship. **DynamicConsentFormBody** contains the structured and free-text sections of the electronic informed consent form and is the primary artifact for communicating terms, risks, and expectations. **DynamicConsentFormActor** is realized through strategy subclasses, including Processor, Custodian, Regulation, and Auditor, representing distinct legal or institutional entities that must endorse or query consent, thereby enforcing multi-party endorsement aligned with stakeholders such as researchers, data custodians, regulators, and ethics bodies. **DynamicConsentData** binds the consent state to a specific study-participant pairing, maintains a consent history list of endorsements, and implements one record per subject–study pair as a sovereignty-preserving structure. Endorsement records who signed, when the signature occurred, and a signature hash, capturing accountability and enabling dispute resolution. **BlockchainRecord** anchors integrity through an on-chain hash, a transaction identifier, and a snapshot of the consent artefact, supporting immutability and audit. **BlockchainProfile** stores ledger credentials and the public key material required for on-chain identity. **DynamicConsentHistory** is exposed as an interface that supports read-oriented governance queries, such as retrieving study consent history, checking consent status by study, and generating consent history reports for oversight actors. **DynamicConsentHistoryRequest** and **DynamicConsentHistoryReport** support compliance reporting by separating request parameters from aggregated reporting views. An abstract dynamic consent actor with ID, name, URI, and address generalizes all legal entities that may sign or query consent, preserving extensibility as new governance stakeholders are introduced.

## 16.5. Communication Aggregate

The communication aggregate supports continuous engagement and traceable discourse between participants and research teams. **Chat** manages a contact list of users and an observable stream to enable ongoing communication in a governed context. **Message** represents the atomic communicative act, including author, receiver, body, and timestamp, enabling traceability and later review. **MessageHistory** provides an archive that can be lazily loaded to reduce overhead while still preserving records for disputes, audits, and accountability. **Notifications** are triggered by **Rule** objects, supporting the right to be informed and the related transparency duties articulated in Section 6.

## 16.6. Anonymized Analytics Aggregate

Anonymized analytics aggregate enables insight while minimizing identifiability. **AnonymizedParticipant** stores coarse demographic buckets and participation states, such as age and gender buckets, reward status, and hashes of dynamic consent history, supporting analytical utility without direct personal identifiers. **AnonymizedStudy** groups cohorts of anonymized participants alongside traits and assets to support population-level analytics and public-health insight while honouring minimization and governance constraints.

## 16.7. Utility and Cross-Cutting Classes

Several cross-cutting classes support review workflows, governance decisions, and accountability across the platform. Comment enables threaded feedback on both study artefacts and dynamic consent forms. **DynamicConsentFormReview** and **StudyReview** capture stateful review processes, recording auditor and principal investigator decisions in a structured and traceable manner. SchemaDecisionMaker encodes substitute decision-maker logic, for example pediatric consent scenarios, ensuring that consent authority can be represented when direct subject consent is not applicable.

## 16.8. How the Class Diagram Reflects Governance Actors

Governance actors are realized directly through the platform's class structure and interfaces. The data subject is represented by Participant, ParticipantAction, and **DynamicConsentData**, enabling self-service

enrolment and reconsent, revocation rights, and governed communication. The researcher is represented by Researcher and **ResearcherAction**, supporting study authoring, cohort management, and analytics requests. Oversight is operationalized through **PrincipalInvestigator** and **PrincipalInvestigatorAction**, which embody accept-or-reject authority over study profiles and broader responsibility for oversight. Ethical vetting is represented by Auditor, **AuditorAction**, and **DynamicConsentFormReview**, enabling formal review of consent artefacts and associated audit responsibilities. Data custodians and third parties are represented by **ThirdParty**, **ThirdPartyAction**, and the custodian dynamic consent actor strategies, supporting consent validation prior to disclosure. The blockchain network is represented by **BlockchainRecord** and **BlockchainProfile**, providing immutable audit trails and zero-trust traceability primitives. Finally, governance committee functions are reflected in Regulation, dynamic consent actors, Rule, and endorsement policy structures that encode organizational policies into enforceable platform behaviour.

# Appendix D

## 17. Propositional Logic Variables Dictionary and Constraints

Study, core record governing lifecycle, approvals, recruitment, and data collection, variables, status {Sn,Sd,Spa,So,Sp,Su,Se}, overall approval {Aa,Ap,Ar}, IRB approval {Ia,Ip,Ir}, PI approval {Pa,Pp,Pr}, recruitment {Ro,Rs}, data collection {Do,Ds}, note, within each group exactly one variable holds at a time. StudySuspension, suspension and resumption marker for an otherwise active study, variables {Su}. StudyVersion, version lineage and governance identifier, variables {Sv}. ParticipantStatus, per participant per study progression, variables {U,Pi,Pe,Pw}. StudyFeedback, participant ratings and comments, variables {Fr,Fc}. DataPrivacy, anonymization and sharing flags plus consent state, variables {Da,Dn,Dshare,Pg,Pr}. StudyOutcome, primary outcome state, variables {Oo,On}. ConflictResolution, dispute lifecycle, variables {Cr,Csol}. DynamicConsentForm, current consent form and its review state, variables {Dd,Dp,Dap}. StudyStatisticsEntity, aggregate counters (non-negative), variables {V,W,I,L,E}, note, context disambiguates from event letters below. StudyTraits, trait or reward value, variables {R}. ConsentTransaction, atomic consent action status per participant per study, variables {CTe,CTw,CTp,CTr}. ConsentPrivacyQuantificationScore, study-level score and benefit framing, variables {CS,PB,SB}. User, user existence and role flags plus permission flags, variables {U,P,R,A,PI,TP,Rc,Rs,Rm,PIr,IRBr,TPc,Pg,Pr}. StudyParticipants, eligibility and demographics policy, variables {G,Amin,Amax,S}. Devices, device metadata, variables {B,M,T}. Assets, study media, variables {L,C,V,VT}. UserInteractionEntity, interaction events, variables {I,E,W,L,V}, note, context disambiguates from statistics counters. NotificationEntity, outbound notification metadata, variables {NT,TT,TB,TG,NI}. ContactListEntity, contact list presence or identifier, variables {CL}. ProfileImage, user profile image presence or identifier, variables {PI}.

Notation macros, ExactlyOne(X1..Xn) means $(X1 \vee \ldots \vee Xn) \wedge \wedge i<j \neg(Xi \wedge Xj)$, implication constraints that describe admissibility of states are interpreted as guard conditions (temporal intent) where

noted by the surrounding text, and “evt” versus “cnt” disambiguates interaction events from counters when symbols overlap.

Complements, recruitment, $Rs \leftrightarrow \neg Ro$ (or $Ro \rightarrow \neg Rs$, $Rs \rightarrow \neg Ro$), data collection, $Ds \leftrightarrow \neg Do$ (or $Do \rightarrow \neg Ds$, $Ds \rightarrow \neg Do$), optional sanity, $(Ro \vee Rs) \wedge \neg(Ro \wedge Rs)$, $(Do \vee Ds) \wedge \neg(Do \wedge Ds)$. Dynamic consent form workflow edges, $Dd \rightarrow Dp$, $Dp \rightarrow Dap$, $Dp \rightarrow Dd$, and pending approval allows pending or approved form, $Spa \rightarrow (Dp \vee Dap)$. Outcome well-formedness, $On \rightarrow \neg Oo$, and on study end, $Se \rightarrow (Oo \vee On)$. Roles imply permissions, $R_role \rightarrow (Rc \wedge Rs_perm \wedge Rm)$, $PI_role \rightarrow PIr$, $TP_role \rightarrow TPc$, $A_role \rightarrow (Rc \wedge Rs_perm \wedge Rm \wedge PIr \wedge IRBr \wedge TPc)$. Event to counter binding, $V_evt \rightarrow V_cnt$, $L_evt \rightarrow L_cnt$, $I_evt \rightarrow I_cnt$, $E_evt \rightarrow E_cnt$, $W_evt \rightarrow W_cnt$.

Study lifecycle and governance, $ExactlyOne(Sn,Sd,Spa,So,Sp,Su,Se)$, $So \rightarrow (Ia \wedge Pa)$, $(Ir \vee Pr) \rightarrow \neg So$, $Spa \rightarrow (Ap \wedge Ip \wedge Pp)$, $(Sp \vee Se) \rightarrow So$ (temporal intent), $Ro \rightarrow So$, $Do \rightarrow So$, $Sd \rightarrow (\neg Ro \wedge \neg Do)$, $Aa \leftrightarrow (Ia \wedge Pa)$, $Sn \rightarrow Sd$, $So \rightarrow (Sd \vee Spa)$ (temporal intent), $Se \rightarrow (So \vee Sp)$ (temporal intent), $Rc \rightarrow Sd$, $Rs \rightarrow Spa$, $Rm \rightarrow (Pg \wedge Pr)$, $PIr \rightarrow (Aa \vee Ar)$, $IRBr \rightarrow (Ia \vee Ir)$, $TPc \rightarrow (Pg \wedge \neg Pr)$.

StudySuspension, $Su \rightarrow So$, and resumption intent, $So \rightarrow Su$. StudyVersion, $Sv \neq \emptyset$, and activation constraint, $Sv \rightarrow (Ia \wedge Pa)$. ParticipantStatus, $Pi \rightarrow U$, $Pe \rightarrow Pi$, $Pw \rightarrow Pe$. StudyFeedback, $(Fr \vee Fc) \rightarrow Pe$, and bounds, $0 \leq Fr \leq 5$. DataPrivacy, $Dshare \rightarrow Da$, $Dshare \rightarrow (Pg \wedge \neg Pr)$, and exclusivity, $\neg(Da \wedge Dn)$. StudyOutcome, $Oo \rightarrow So$, and $ExactlyOne(Oo,On)$. ConflictResolution, $Cr \rightarrow So$, $Csol \rightarrow Cr$. DynamicConsentForm state, $(Spa \vee So) \rightarrow Dap$, and $ExactlyOne(Dd,Dp,Dap)$. StudyStatisticsEntity, $StudyCreated \rightarrow (V \geq 0 \wedge W \geq 0 \wedge I \geq 0 \wedge L \geq 0 \wedge E \geq 0)$. StudyTraits, $\neg Sd \rightarrow (R \geq 0)$. ConsentTransaction, $(CTe \vee CTw) \rightarrow So$, $Se \rightarrow (\neg CTp \wedge \neg CTr)$, and $ExactlyOne(CTe,CTw,CTp,CTr)$. CPIQ completeness, $So \rightarrow (CS \geq 0 \wedge PB \wedge SB)$. User and role coupling, $(CTe \vee CTw \vee CTp \vee CTr) \rightarrow (U \wedge P)$, $CTe \rightarrow So$, $CTw \rightarrow So$, $Rc \rightarrow Sd$, $Rs \rightarrow Spa$, $Rm \rightarrow (Pg \wedge Pr)$, $PIr \rightarrow (Aa \vee Ar)$, $IRBr \rightarrow (Ia \vee Ir)$, $TPc \rightarrow (Pg \wedge \neg Pr)$. StudyParticipants eligibility, $G \in \{male,female,other,both,all\}$, $Amin \leq Amax$. Devices completeness, $(B \neq \emptyset) \wedge (M \neq \emptyset) \wedge (T \neq \emptyset)$. Assets completeness, $(L \neq \emptyset) \wedge (C \neq \emptyset) \wedge (V \neq \emptyset) \wedge (VT \neq \emptyset)$. UserInteractionEntity validity, $(I \vee E \vee W \vee L \vee V) \rightarrow U$. NotificationEntity completeness, $(NT \neq \emptyset) \wedge$

$(TT \neq \emptyset) \wedge (TB \neq \emptyset) \wedge (TG \neq \emptyset) \wedge (NI \neq \emptyset)$. ContactListEntity presence, $CL \neq \emptyset$. ProfileImage presence, $PI \neq \emptyset$.

# Appendix E

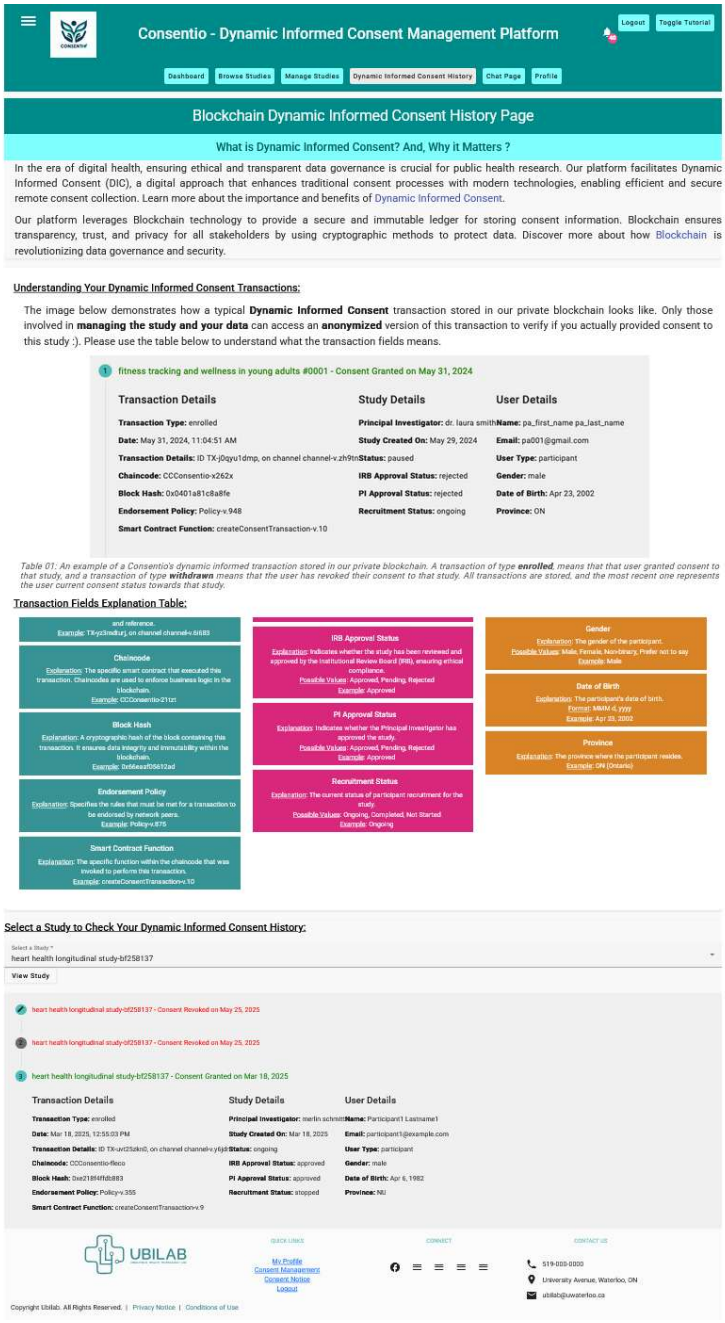
# 18. Consentio Platform User Interface Screenshots

This appendix documents the main Consentio user interface screens captured during development and evaluation of the dynamic informed consent platform. The screenshots are organized as numbered subsections so that participant-facing, researcher-facing, governance, communication, analytics, and ledger-backed consent-history components can be referenced individually. Each subsection provides a brief description of the screen's purpose and places the figure caption above the corresponding image for thesis-style appendix formatting.

## 18.1. Blockchain Dynamic Informed Consent History Page

This screen documents the participant-facing consent history view and explains how blockchain consent transactions are represented through transaction details, study metadata, and user details. It supports transparency by showing how consent events can be reviewed and interpreted after they are recorded.

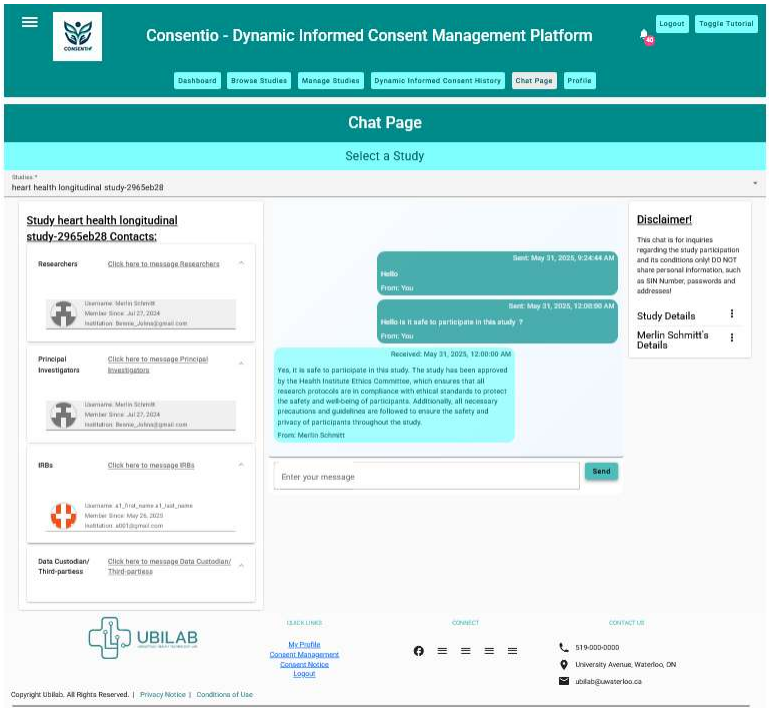
*Figure .1 - Blockchain Dynamic Informed Consent History Page.*



## 18.2. Chat Page and Study Conversation UI

This screen presents the study-specific chat interface, where participants can communicate with researchers, principal investigators, IRB contacts, and data custodians. The layout combines role-based contacts, a message thread, and contextual study details to support accountable communication.

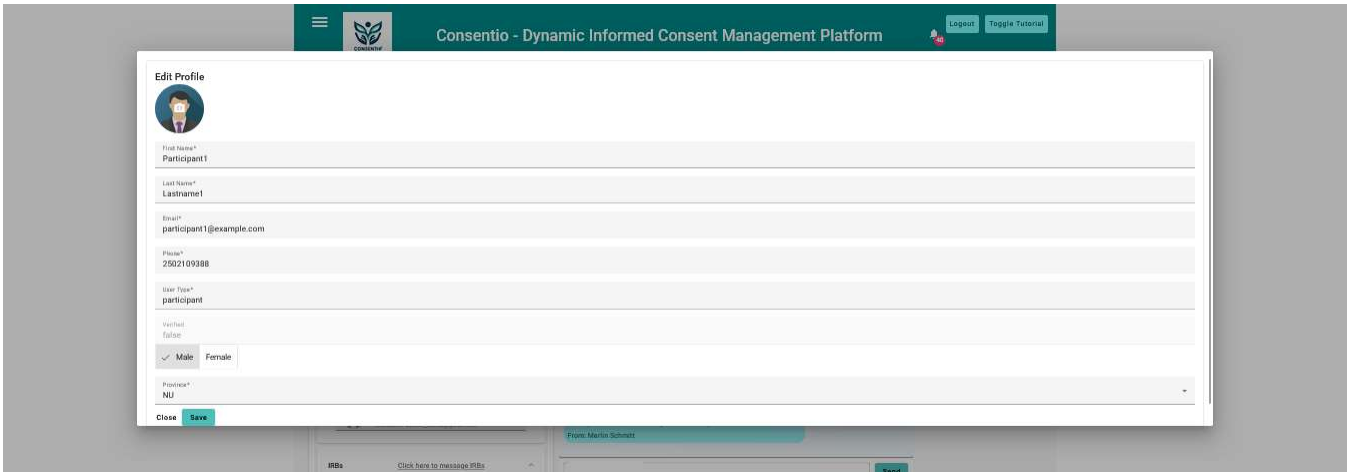
*Figure 2 - Chat Page and Study Conversation UI.*



## 18.3. Researcher Identity Modal

This modal provides a compact researcher identity view for the selected study. It helps participants verify who is associated with a study without requiring them to leave the current workflow.

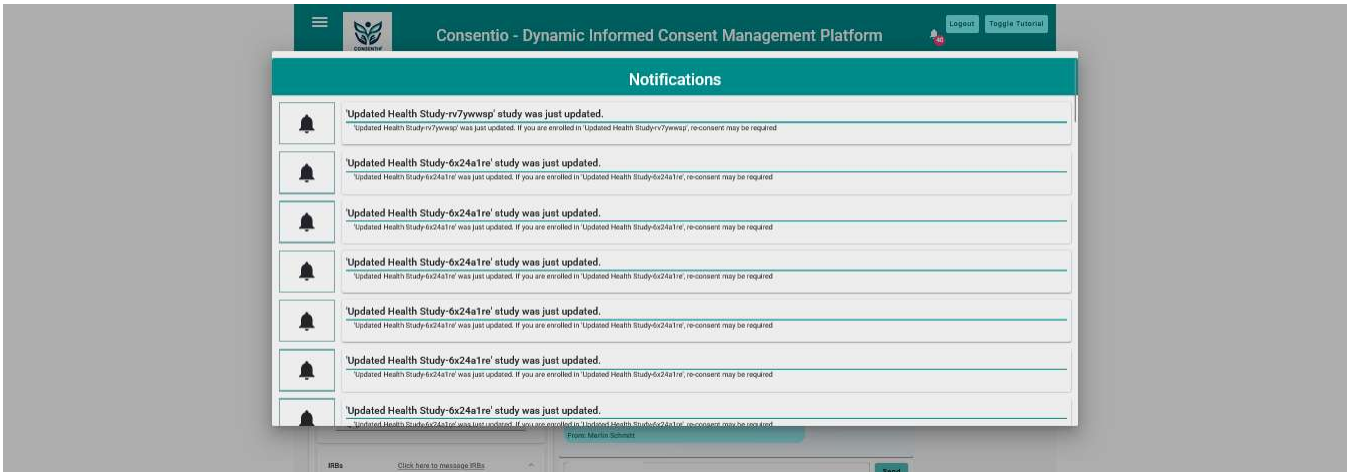
*Figure 3 - Researcher Identity Modal.*



## 18.4. Study Metadata Modal

This modal summarizes study metadata in a focused dialog. It supports quick inspection of study information, status, and related governance fields while preserving the participant's place in the interface.

*Figure.4 - Study Metadata Modal.*



## 18.5. Researcher Dashboard Analytics Overview

This screen shows the researcher analytics dashboard with study status tables and engagement metrics. It supports research management by making approvals, enrolment, withdrawals, and participant activity visible in a consolidated view.

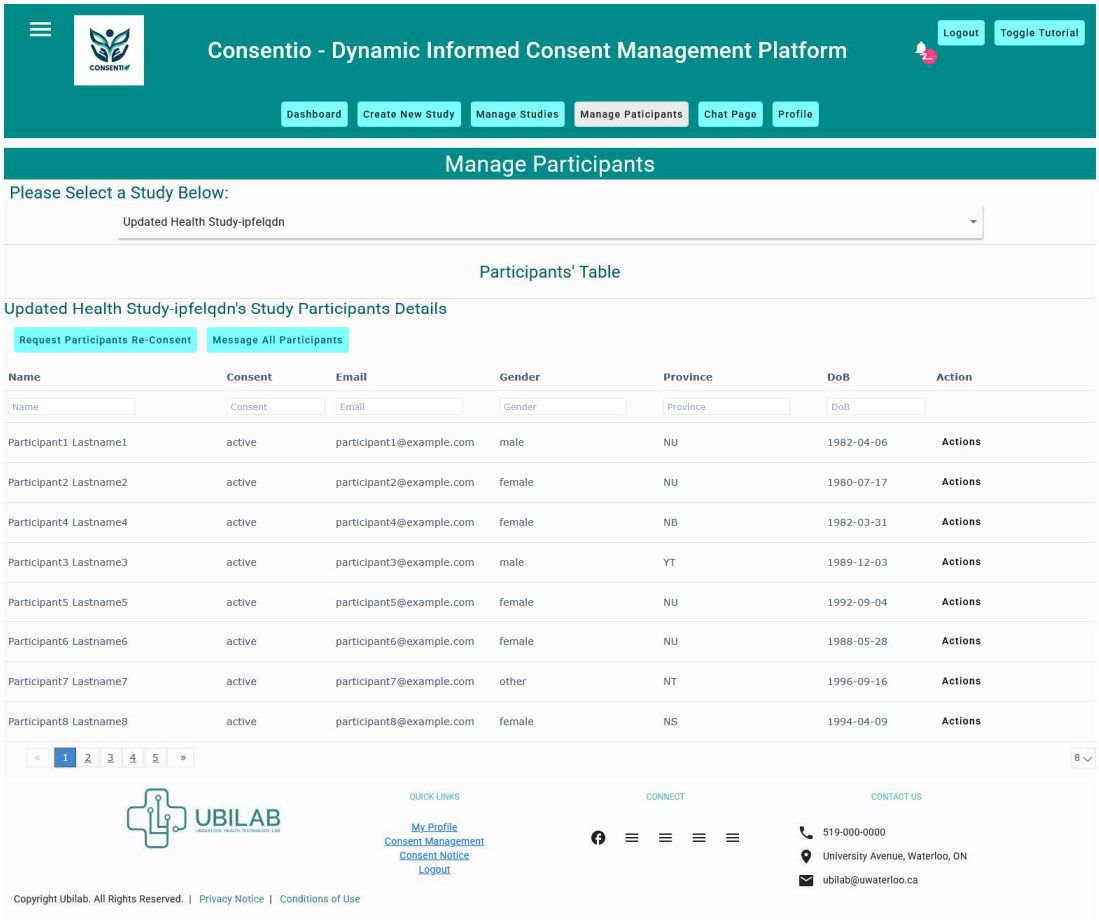
*Figure 5 - Researcher Dashboard Analytics Overview.*



## 18.6. Participant Management Page

This screen shows the participant management interface used by researchers to review participant-level study activity. The page provides a table-based workflow for monitoring participant status and managing study participation records.

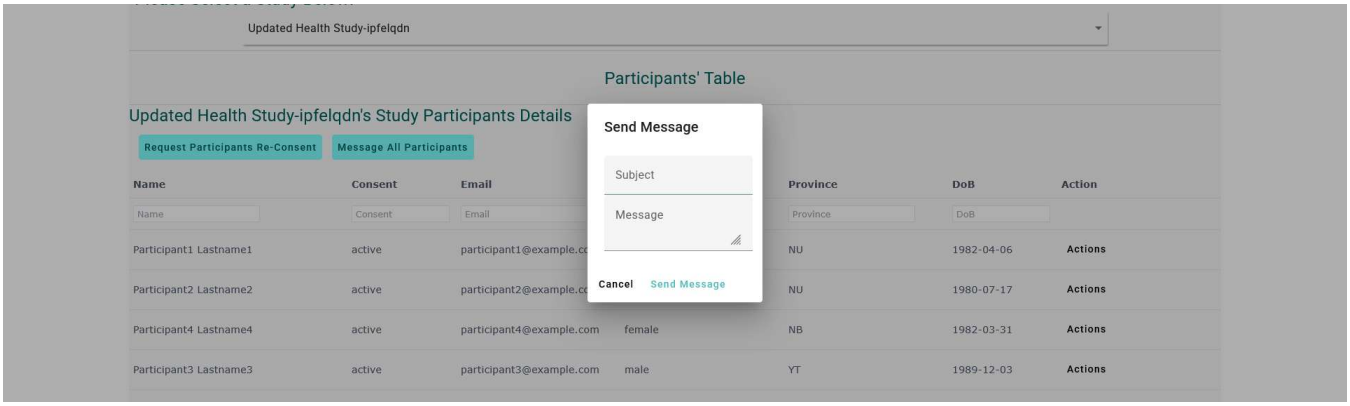
*Figure 6 - Participant Management Page.*



## 18.7. Message Participants Modal

This modal enables researchers to send messages to participants from within the participant management workflow. It supports targeted communication and study follow-up while keeping the interaction connected to the selected study context.

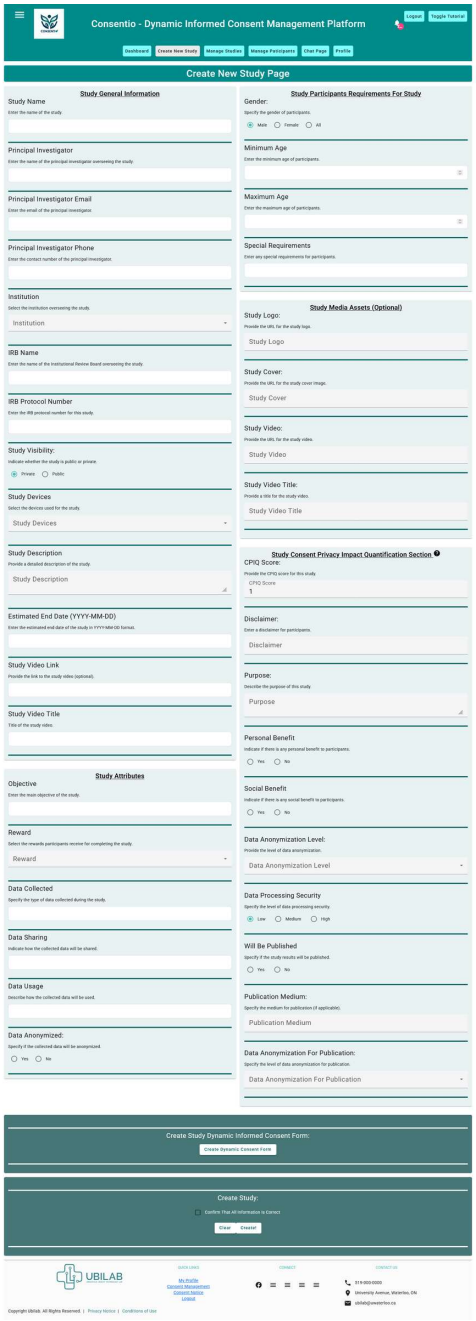
*Figure 7 - Message Participants Modal.*



## 18.8. Researcher Study Management and Lifecycle Control Page

This screen presents the researcher-facing study management workflow, including study status information, governance-related sections, and lifecycle controls. It supports operational oversight of studies after creation and during active management.

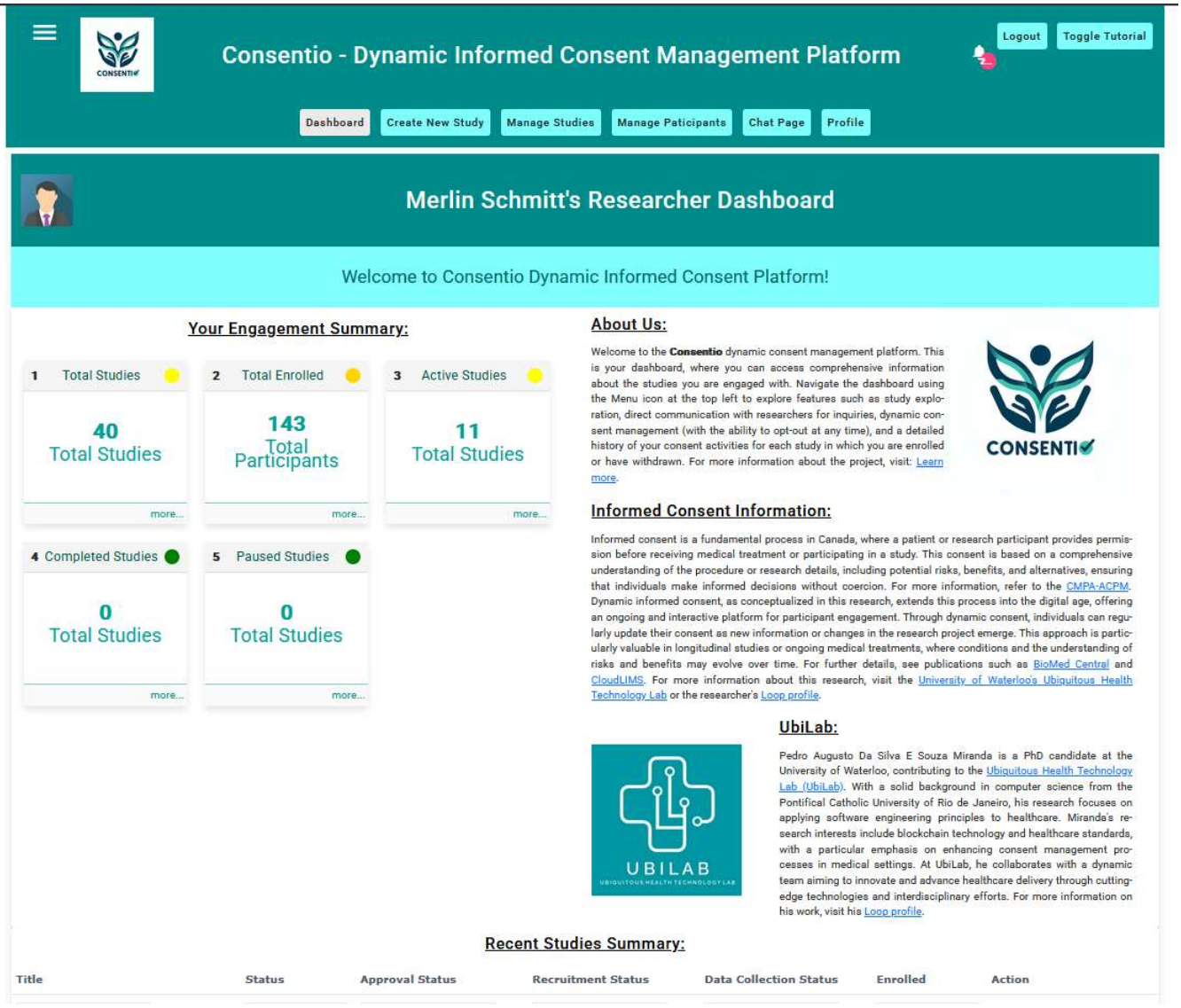
*Figure .8 - Researcher Study Management and Lifecycle Control Page.*



## 18.9. Researcher Dashboard Home UI

This screen provides a high-level researcher dashboard with totals for studies, participants, withdraws, and wishlists. It introduces the researcher to current platform activity and recent study summaries.

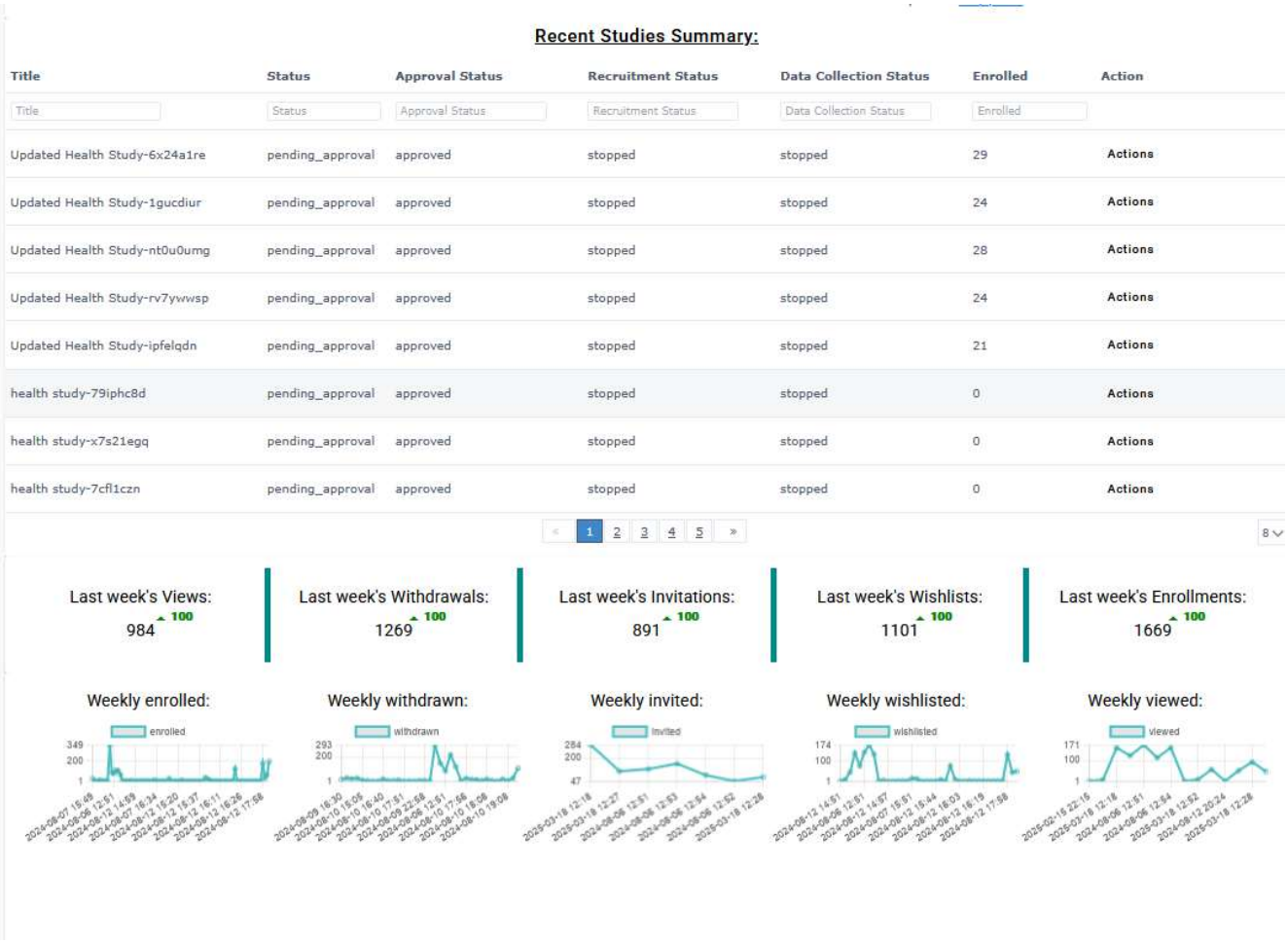
*Figure .9 - Researcher Dashboard Home UI.*



## 18.10. Recent Studies and Engagement Metrics UI

This screen expands the dashboard summary with recent study records, latest participant actions, and compact trend indicators. It helps researchers identify engagement patterns across their active study portfolio.

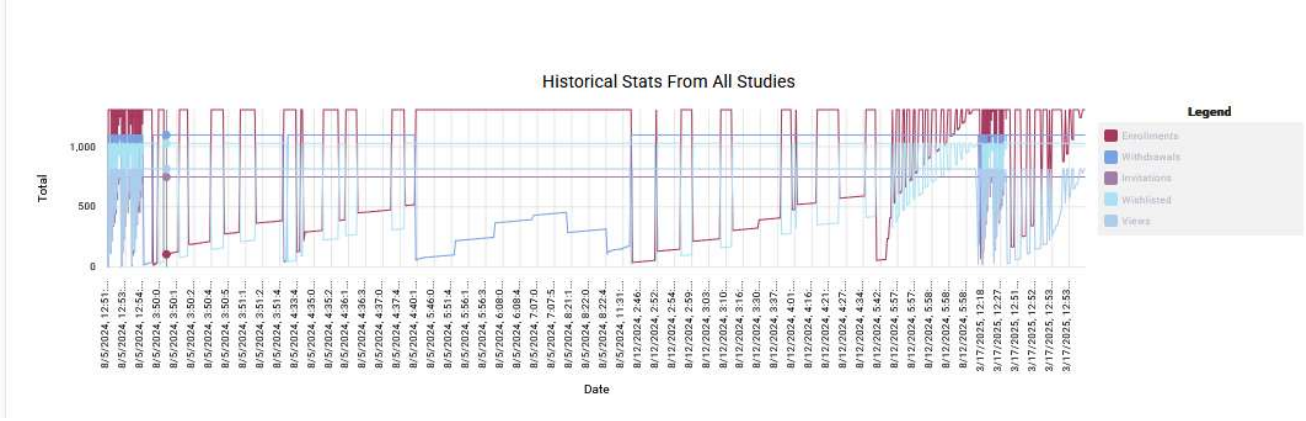
*Figure .10 - Recent Studies and Engagement Metrics UI.*



## 18.11. Historical Consent and Engagement Line Chart

This chart view presents historical activity trends across studies. It supports longitudinal monitoring by showing how enrolment and engagement metrics change over time.

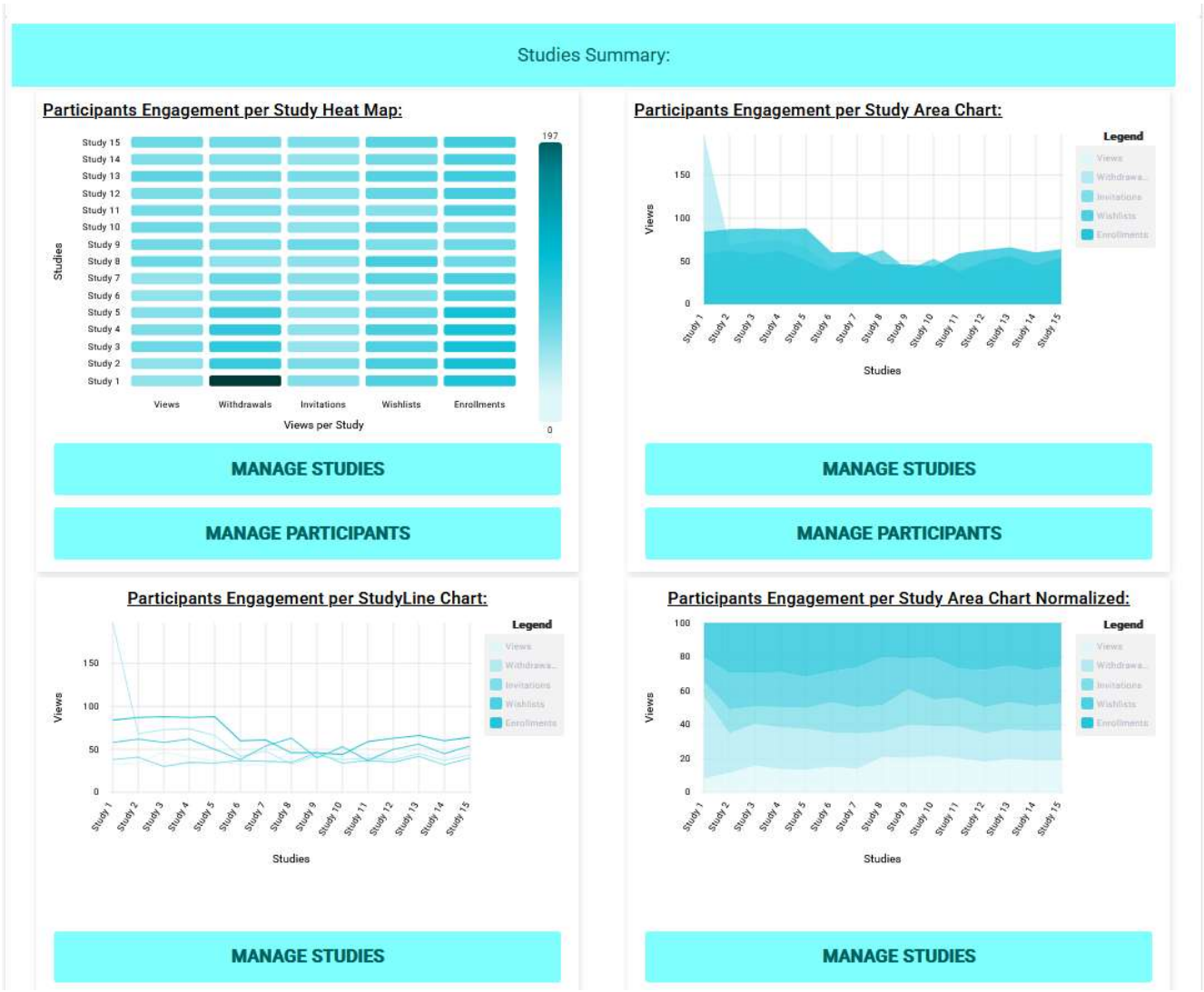
*Figure .11 - Historical Consent and Engagement Line Chart.*



## 18.12. Study Summary Analytics Dashboard UI

This dashboard section presents multiple study-level analytics, including enrolment trends, job or task engagement, and participant outcomes. It supports rapid review of study performance indicators from a single page.

*Figure .12 - Study Summary Analytics Dashboard UI.*



## 18.13. Enrollment and Participant Trend Analytics UI

This screen continues the analytics view with participant trends and invitation or enrolment patterns. It helps researchers compare activity across studies and identify where follow-up may be needed.

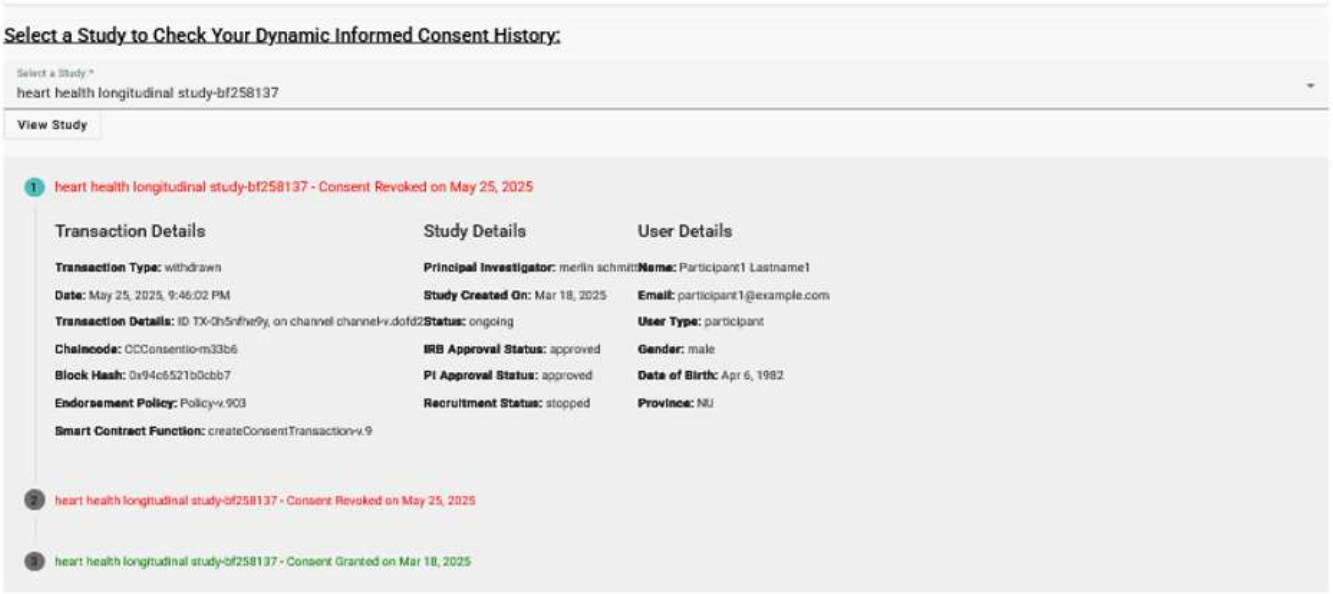
*Figure .13 - Enrollment and Participant Trend Analytics UI.*



## 18.14. Consent History Transaction Detail UI

This screen shows a selected consent transaction with transaction details, study details, and user details. It illustrates how Consentio can provide a participant-readable record of consent status and provenance.

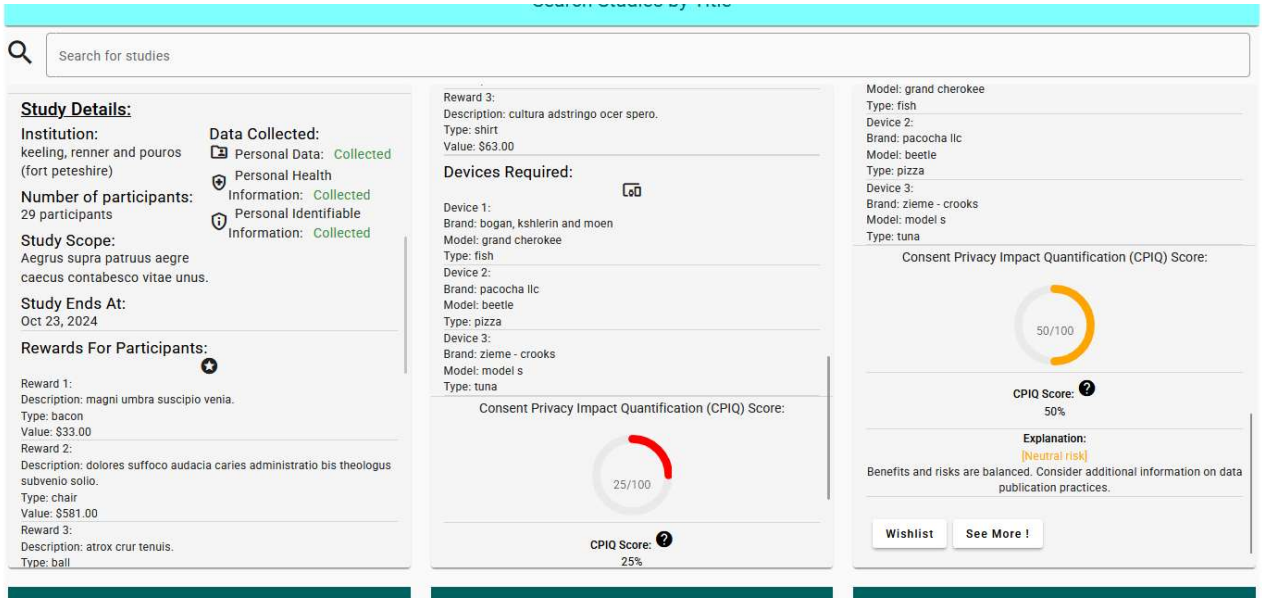
*Figure .14 - Consent History Transaction Detail UI.*



## 18.15. Browse Studies Grid UI

This screen shows the participant-facing browse studies interface, where available public health studies are displayed as cards. Each card summarizes the study title, description, metadata, and consent-related actions such as viewing details or saving the study.

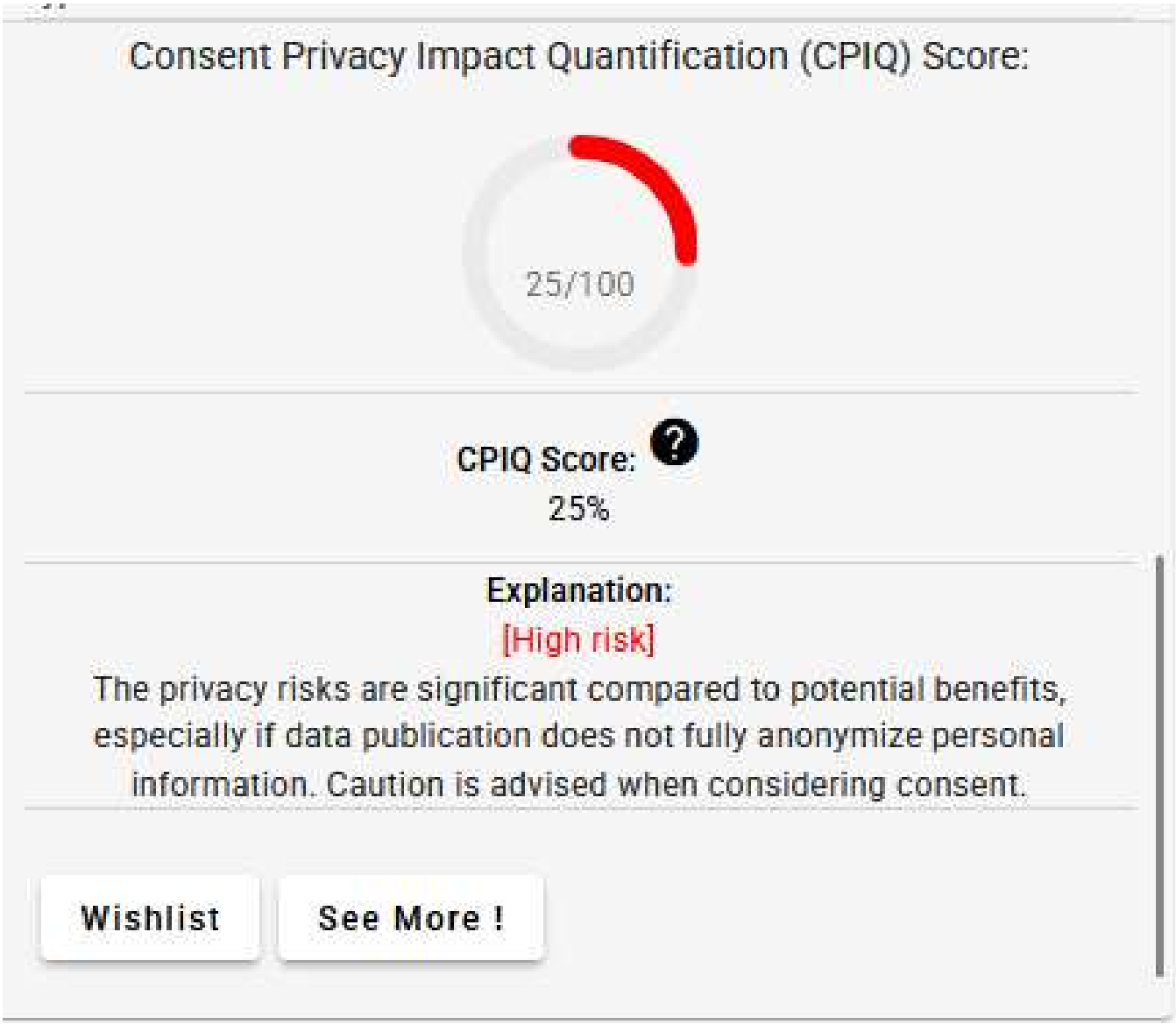
*Figure .15 - Browse Studies Grid UI.*



### 18.16. CPIQ High-Risk Score Card

This image shows the Consent Privacy Impact Quantification score card for a high-risk scenario. The visual risk indicator communicates that the study may involve greater privacy concerns and encourages caution before consent.

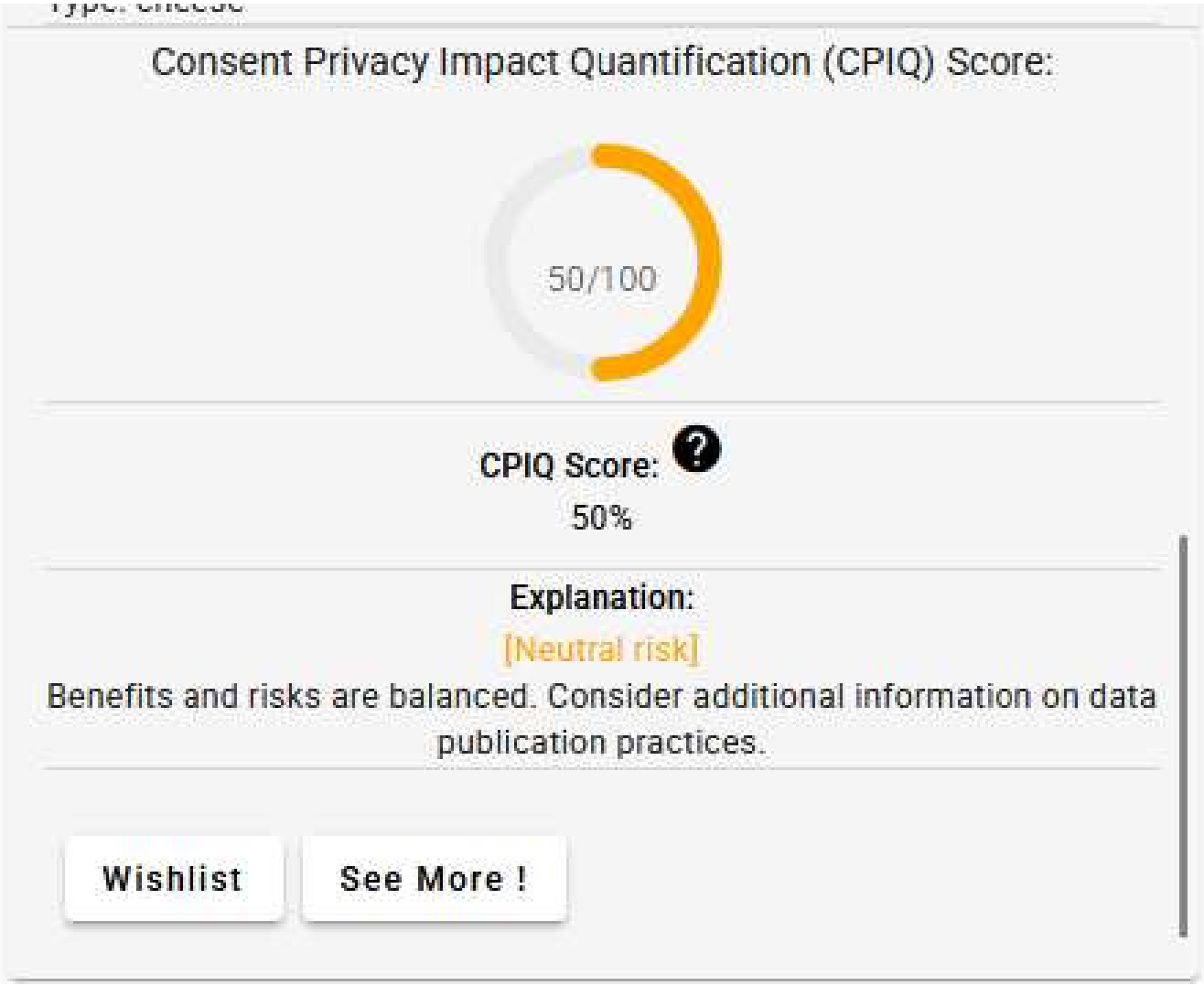
*Figure .16 - CPIQ High-Risk Score Card.*



## 18.17. CPIQ Neutral-Risk Score Card

This image shows the Consent Privacy Impact Quantification score card for a neutral-risk scenario. It communicates a balanced relationship between study benefits and privacy considerations.

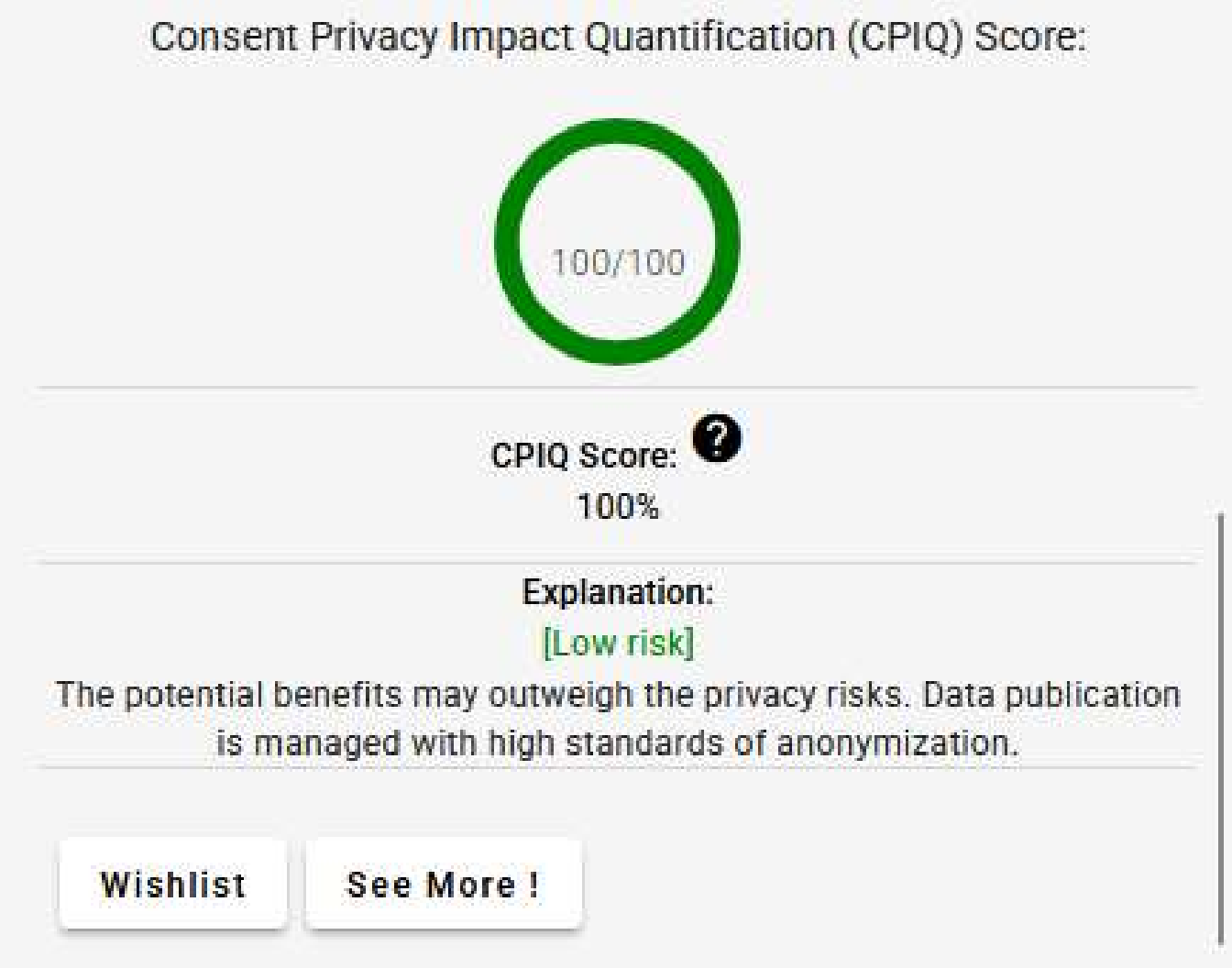
*Figure .17 - CPIQ Neutral-Risk Score Card.*



## 18.18. CPIQ Low-Risk Score Card

This image shows the Consent Privacy Impact Quantification score card for a low-risk scenario. The visual indicator communicates that the potential study benefits outweigh privacy concerns under the stated conditions.

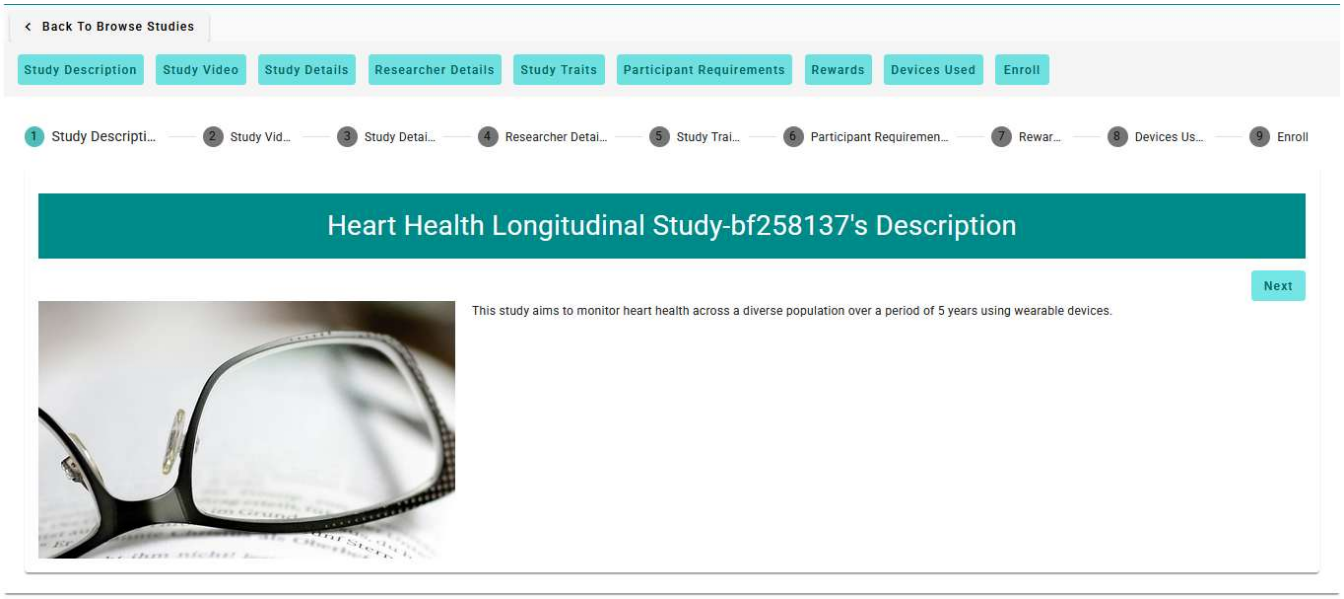
*Figure .18 - CPIQ Low-Risk Score Card.*



## 18.19. Study Description UI

This screen presents the study profile description tab. It provides participants with a study overview, visual context, and navigation steps used to move through the consent review process.

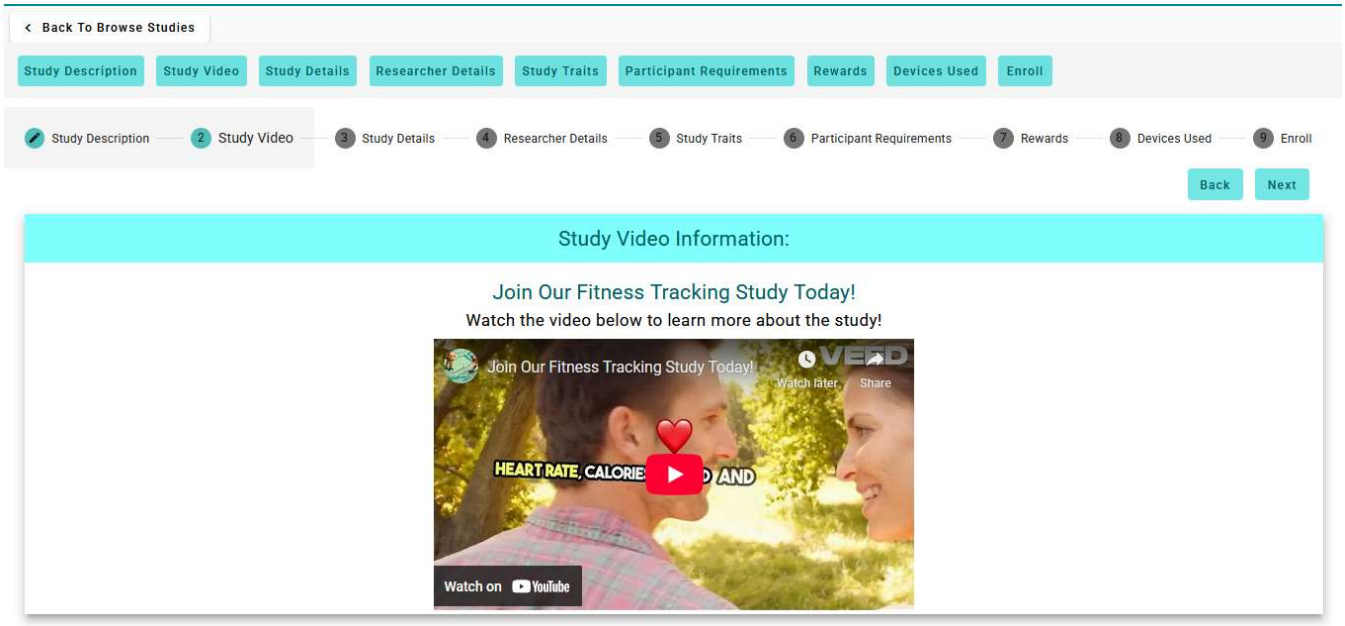
*Figure .19 - Study Description UI.*



## 18.20. Study Video UI

This screen presents the study video tab, where multimedia material can be used to explain the study. The design supports layered disclosure by allowing participants to review information in a format beyond plain text.

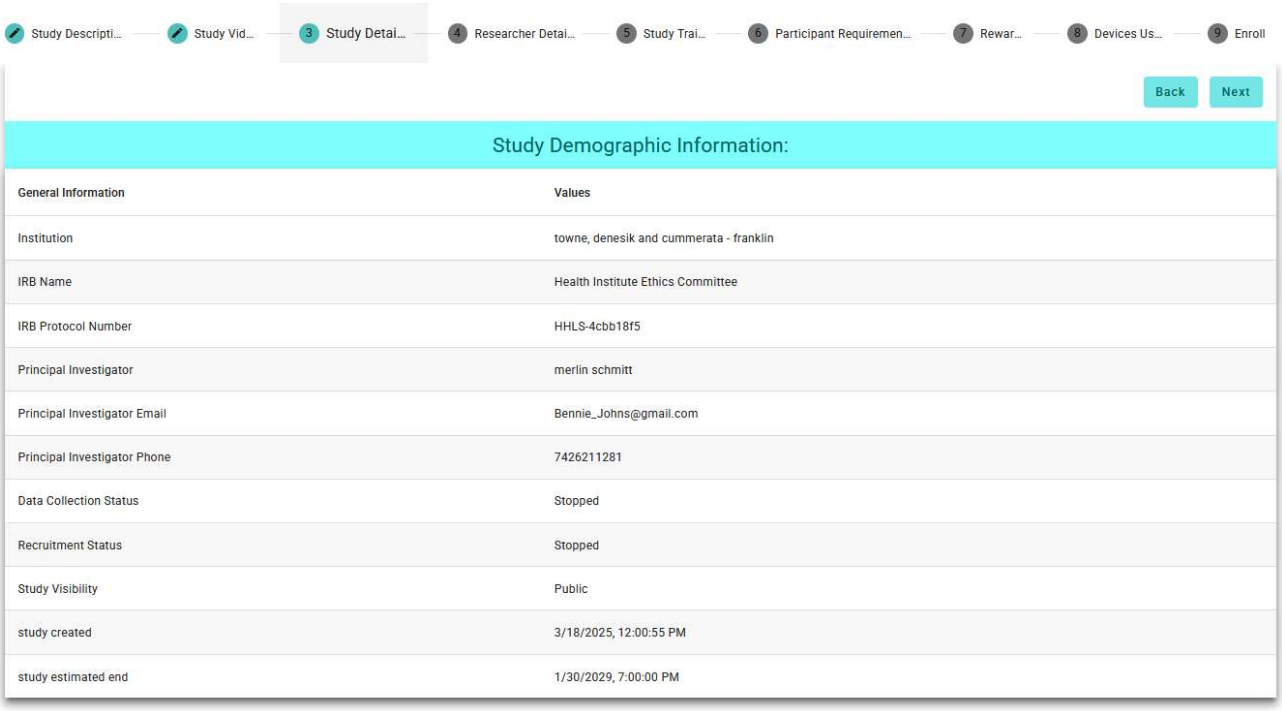
*Figure .20 - Study Video UI.*



## 18.21. Study Details UI

This screen presents structured study details, including study identifiers, dates, topic categories, and other descriptive fields. It supports informed decision-making by making study metadata visible before enrolment.

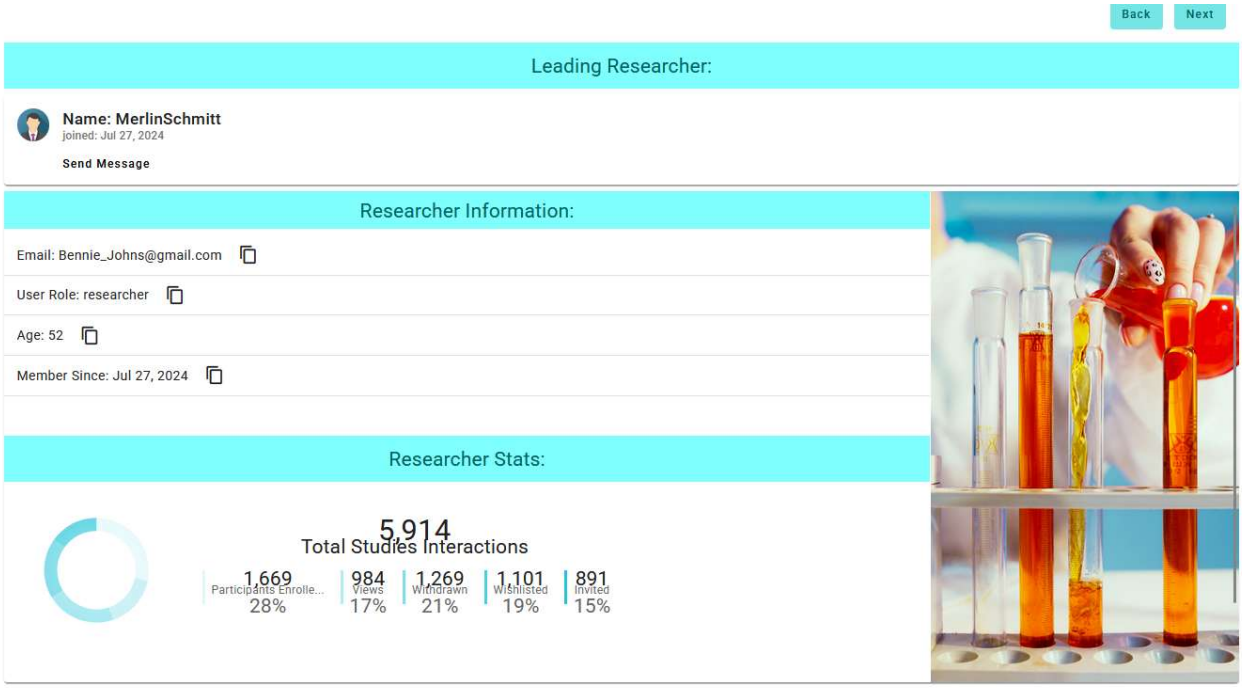
*Figure .21 - Study Details UI.*



## 18.22. Researcher Details and Statistics UI

This screen presents information about the lead researcher and related researcher statistics. It provides contextual transparency about the research team and their role in the study.

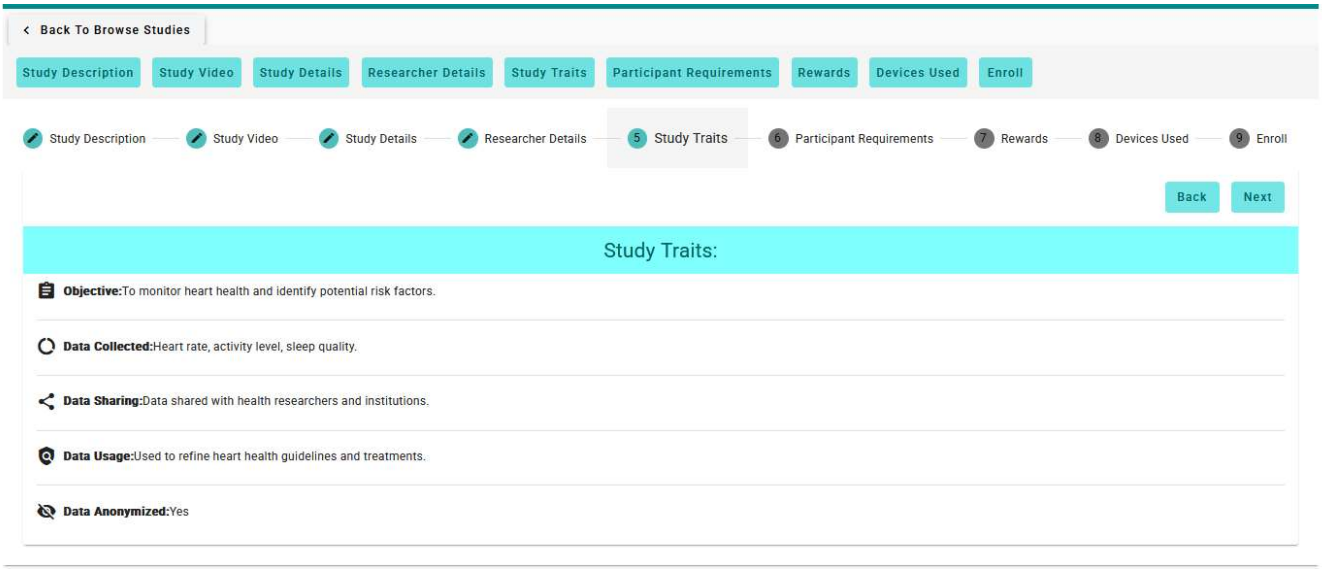
*Figure .22 - Researcher Details and Statistics UI.*



## 18.23. Study Traits UI

This screen lists study traits and characteristics relevant to participant review. It helps translate study properties into a structured format that can be scanned before consent.

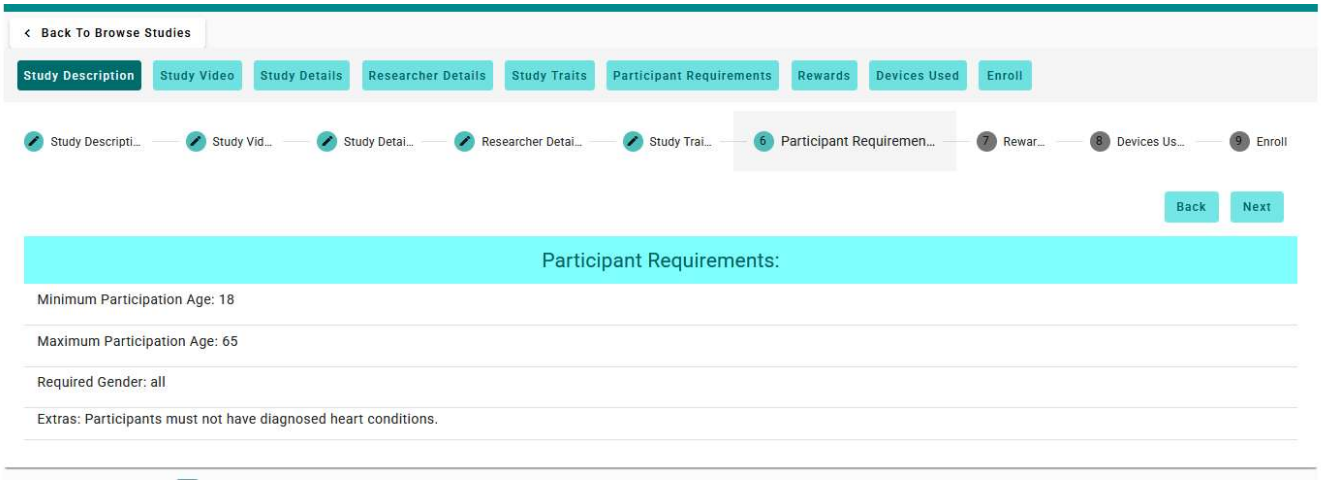
*Figure .23 - Study Traits UI.*



## 18.24. Participant Requirements UI

This screen presents the participant requirements for a study, including age, membership, or enrolment-related criteria. It helps participants determine whether they are eligible and what conditions apply.

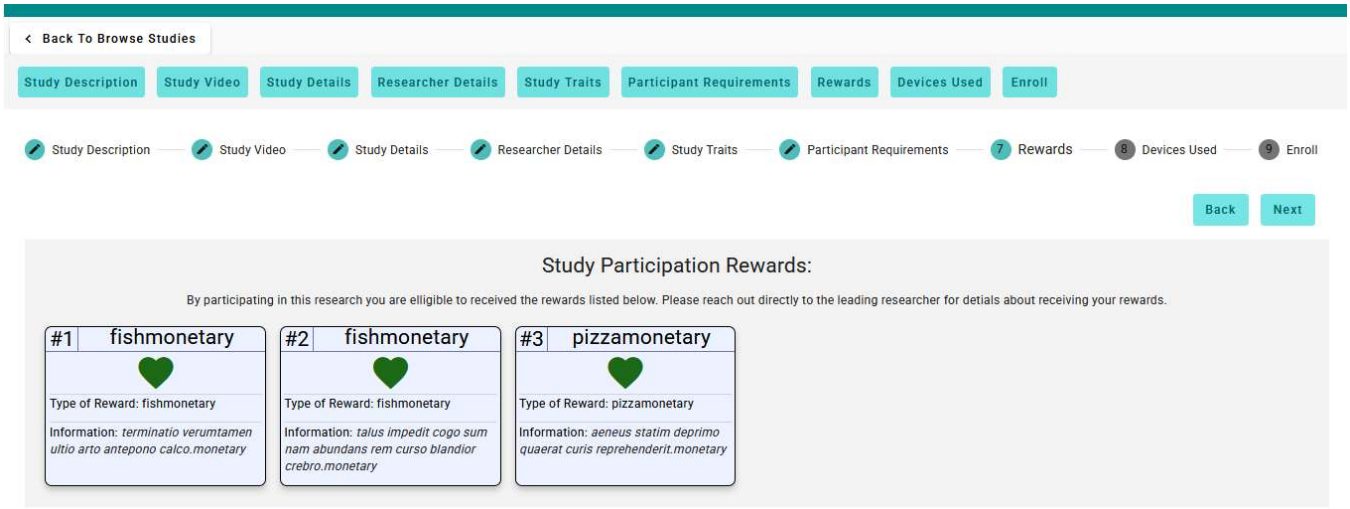
*Figure .24 - Participant Requirements UI.*



## 18.25. Study Rewards UI

This screen presents the reward section of the study profile. It explains participant incentives and distinguishes possible reward categories in a structured interface.

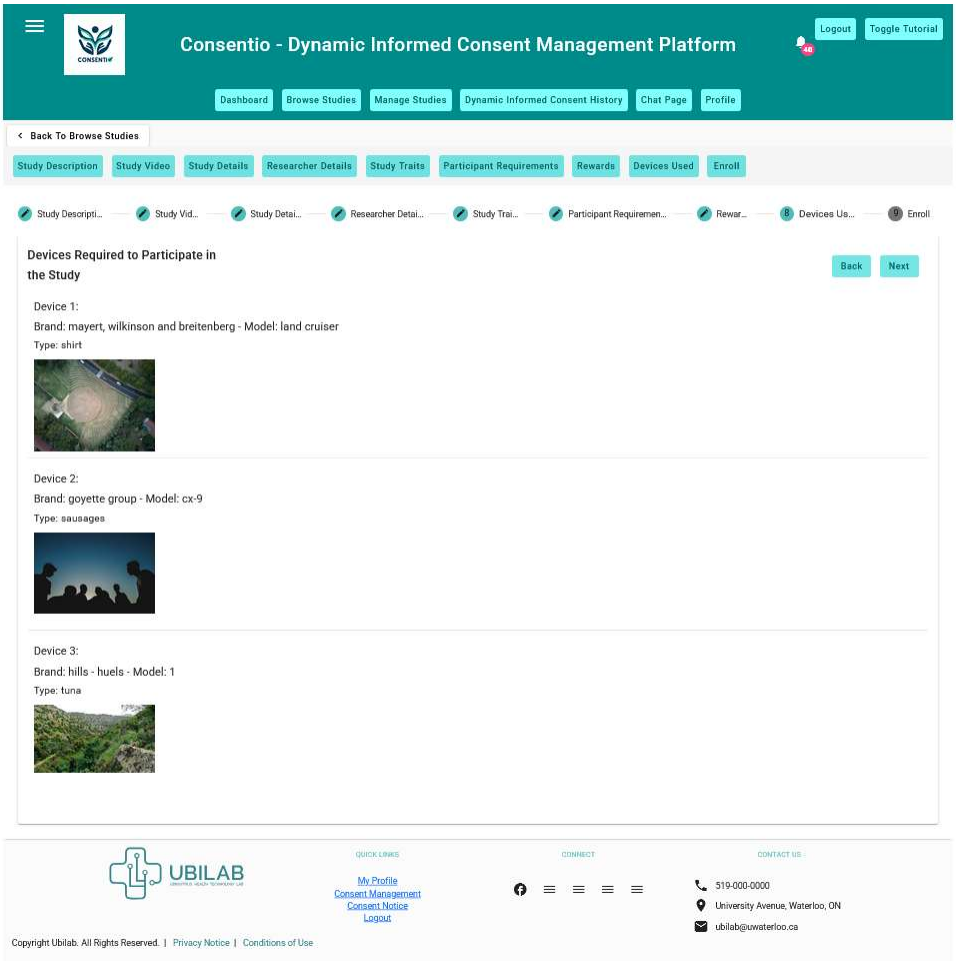
*Figure .25 - Study Rewards UI.*



## 18.26. Devices Used and Study Assets UI

This screen presents devices and study assets associated with the study. It helps participants understand what devices, data sources, or resources are involved in the research process.

*Figure .26 - Devices Used and Study Assets UI.*



## 18.27. Consent Withdrawal Blockchain Transaction Script

This image shows a blockchain transaction script or console output related to consent withdrawal. It illustrates the technical record generated when a participant revokes consent and the action is written to the ledger-backed audit layer.

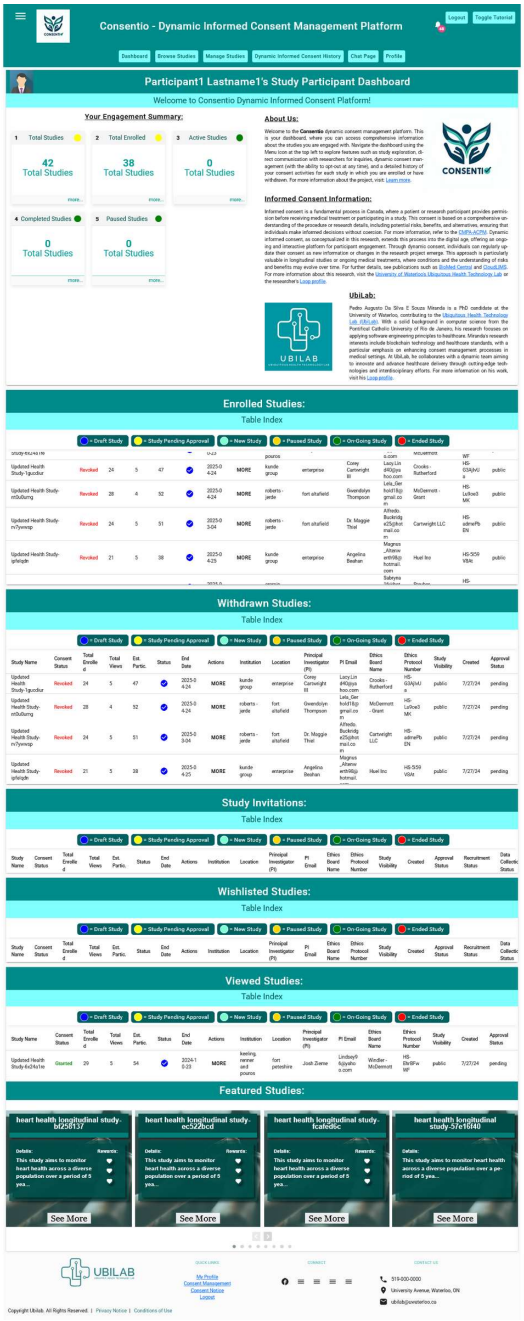
*Figure .27 - Consent Withdrawal Blockchain Transaction Script.*



## 18.28. Participant Dashboard UI

This screen shows the participant dashboard, including totals for active, completed, paused, and withdrawn studies, as well as enrolled, withdrawn, invited, wishlisted, viewed, and featured studies. It centralizes participation status and supports ongoing consent management.

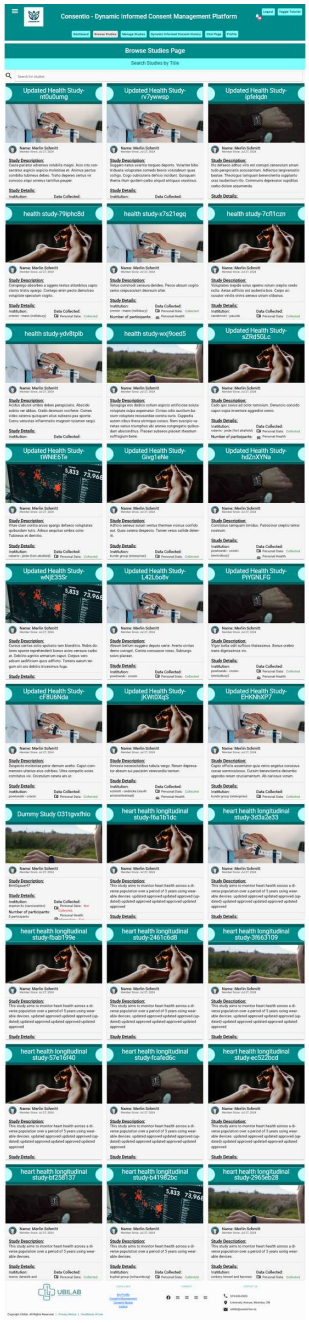
*Figure .28 - Participant Dashboard UI.*



## 18.29. Browse Studies Expanded Catalog UI

This screen presents an expanded browse studies catalog with multiple study cards. It demonstrates how participants can compare available studies and access study descriptions, metadata, and consent-related actions from a single grid.

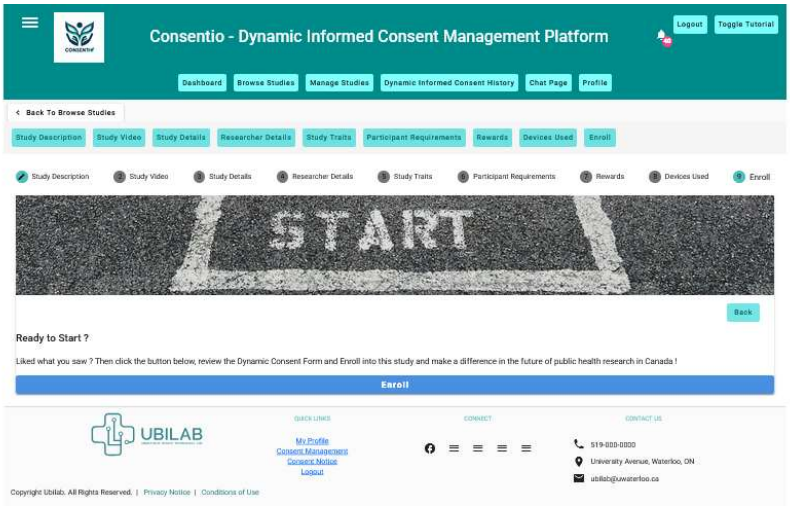
*Figure .29 - Browse Studies Expanded Catalog UI.*



## 18.30. Enrollment Call-to-Action UI

This screen shows the enrolment stage of the study profile workflow. It presents the final call to action for participants to review the dynamic consent form and proceed with enrolment.

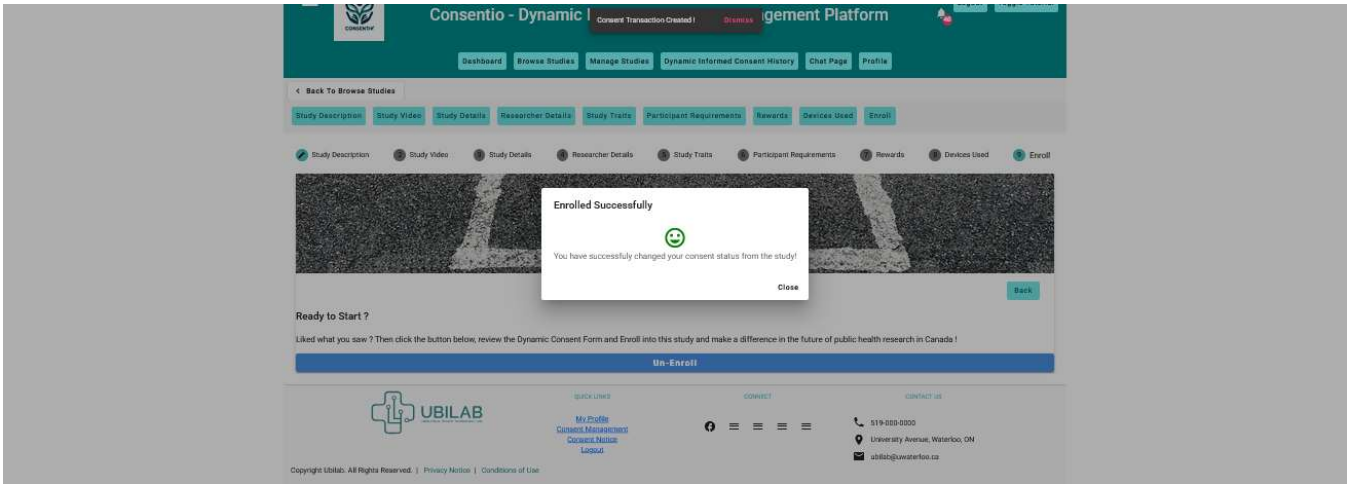
*Figure .30 - Enrollment Call-to-Action UI.*



## 18.31. Enrollment Confirmation Modal UI

This modal confirms successful enrolment and indicates that a consent transaction has been created. It provides immediate feedback that the participant's consent status has changed.

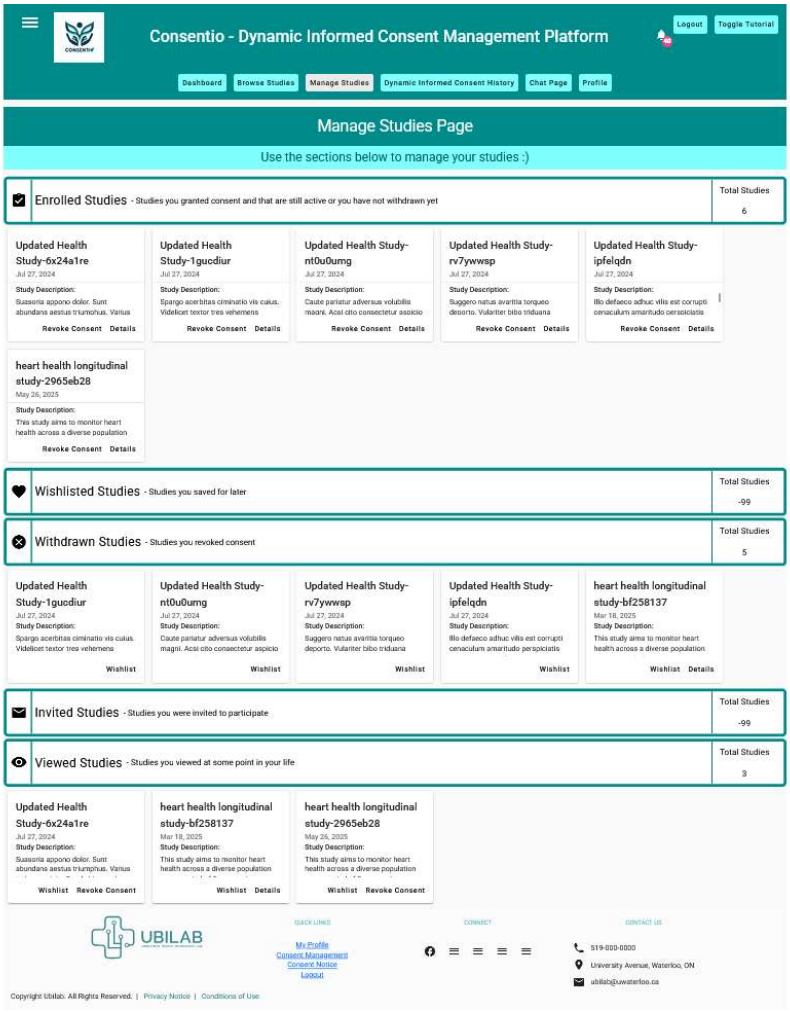
*Figure .31 - Enrollment Confirmation Modal UI.*



## 18.32. Manage Studies Page

This screen shows the participant-facing manage studies page, organizing enrolled, wishlisted, withdrawn, invited, and viewed studies. It supports participant control by making study status and follow-up actions visible.

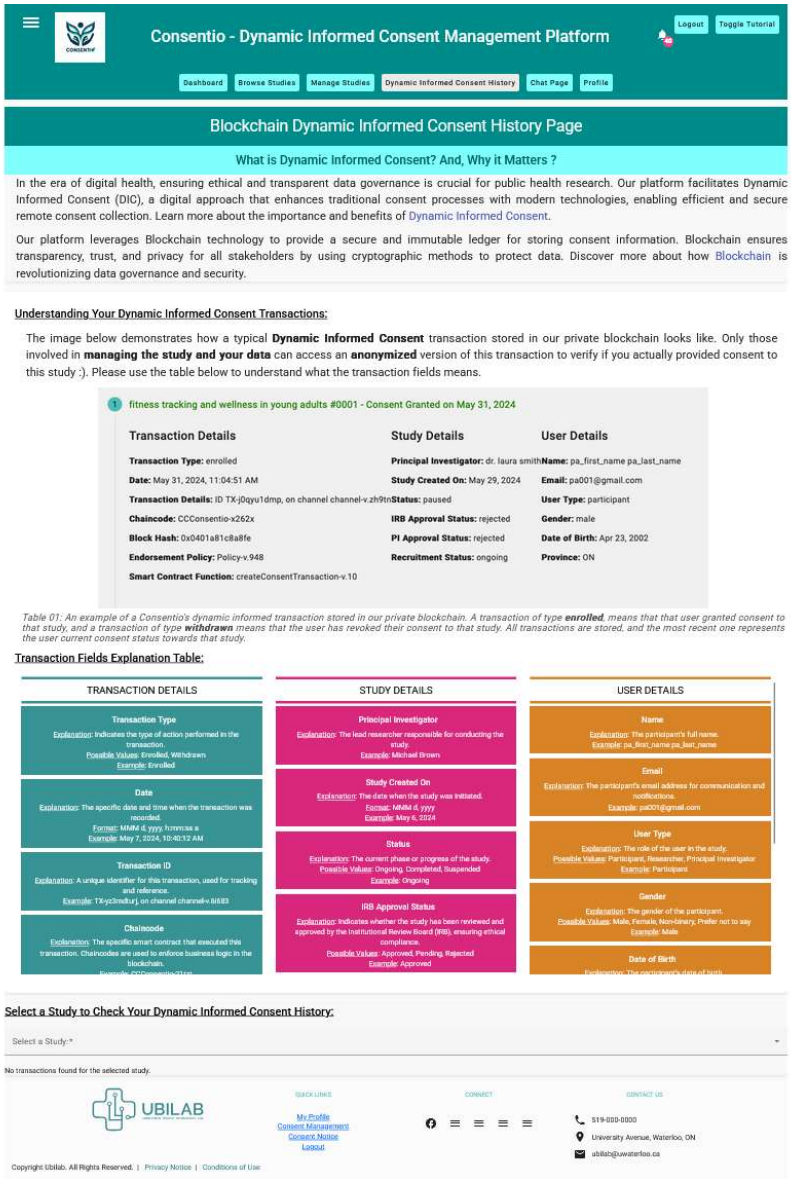
*Figure 32 - Manage Studies Page.*



## 18.33. Dynamic Informed Consent History Page with Transaction Explanation

This screen presents the dynamic consent history page with explanatory material, example transaction fields, and a selected study history view. It connects blockchain auditability to participant-readable consent records.

*Figure 33 - Dynamic Informed Consent History Page with Transaction Explanation.*



# Appendix F

## 19. Governance to Requirements Matrix

This appendix presents a table that maps the governance guideline to the platform's features, constraints, and interfaces.

*Table 28 - Governance-to-implementation traceability matrix.*

| ID | Section 6 Governance Source | Derived Requirement (Section 7) | Design Artifact Mapping (Section 7) | Implementation Component (Consentio) | Verification/ Acceptance |
|---|---|---|---|---|---|
| GOV-01 | IODG framework empowers data subjects while facilitating researchers' PHI access; components, entities, and transactions defined; GDPR considered. | Implement Dynamic Informed Consent (DIC) with fine-grained preferences, real-time re-consent, and participant dashboards. | Use case: Manage Consent; Classes: User, ConsentTransaction, DynamicConsentForm, Study; State diagram: Consent states; Logic: Dshare → (Pg ∧ ¬Pr); Interface: Participant Portal. | Consent service; Preference engine; Notification service. | Unit tests on consent transitions; ledger audit; usability tests on participant control. |
| GOV-02 | Transactions defined via Governance Analytical Framework (GAF): negotiation, directive, reciprocity, distribution; nodal points guide interactions. | Model role-based workflows reflecting directives (IRB/PI), negotiations (DSA), reciprocity (benefits), and distribution (results/data). | Use case: Submit Study for Approval; Classes: Study, IRB, PI, DSA; State diagram: Study approval; Logic: Spa → (Ap ∧ Ip ∧ Pp); Interface: Researcher + IRB/PI views. | Approval workflow service; DSA registry; Policy engine. | Scenario tests for each transaction type; traceable approvals in logs. |
| GOV-03 | Actors and abstract actors identified (data subjects, researchers, IRBs, companies, IODG committee, regulators). | Implement role-based access control (RBAC) and UI segmentation for participants, researchers, PIs/IRBs, auditors, and third-parties. | Use case: Actor login + role dashboards; Classes: Role, Permission; State diagram: Session; Logic: role permissions (PIr, IRBr, TPc); Interface: Role-specific portals. | AuthN/AuthZ service; Angular role modules. | Pen tests for privilege escalation; unit tests for permission checks. |
| GOV-04 | Legal and ethical compliance (e.g., GDPR) is mandated; IRB safeguards biomedical research and participant rights. | Embed compliance checks and consent provenance; ensure IRB review gates prior to recruitment/data collection. | Use case: IRB/PI Approve Study; Classes: Approval, IRBDecision, PIDecision; State: Submitted → Approved; Logic: So → (Ia ∧ Pa); Interface: IRB/PI panels. | Compliance validator; Approval microservice. | Compliance checklist; test that So cannot be reached without approvals. |
| GOV-05 | Data sharing requires DSAs between stakeholders due to heterogeneous infrastructures and policies. | Represent DSAs as machine-readable policies linked to studies and data sources; enforce at access time. | Use case: Create/Attach DSA; Classes: DSA, DataSource; State: DSA Draft → Active; Logic: Dshare → Da; Interface: DSA editor. | Policy store; Access gateway. | Policy evaluation tests; deny-by-default without a valid DSA. |

| ID | Section 6 Governance Source | Derived Requirement (Section 7) | Design Artifact Mapping (Section 7) | Implementation Component (Consentio) | Verification/ Acceptance |
|---|---|---|---|---|---|
| GOV-06 | The framework recommends DIC to give subjects continuous control and transparency. | Support granular toggles (purpose, device, timeframe); revoke at any time; notify stakeholders of changes. | Use case: Update Consent Preference; Classes: ConsentPreference; State: Active ↔ Revoked; Logic: TPc → (Pg ∧ ¬Pr); Interface: Consent settings. | Preference API; Event bus; Notification service. | End-to-end tests: revoke halts data flow; audit notification delivery. |
| GOV-07 | GAF stresses mapping of nodal points and processes across stakeholders. | Define state machines for Study and Consent; instrument transitions with audit logs and reasons. | Use case: Pause/Resume/End Study; Classes: StudyState; State: New → Draft → Pending → Ongoing → {Paused \| Ended}; Logic: (Sp ∨ Se) → So; Interface: Study admin. | State engine; Audit logger. | State-transition coverage; invariants enforced in tests. |
| GOV-08 | Transparency and auditability are essential; ledger-based immutability is highlighted. | Record key transactions (approvals, consent changes, data-sharing) on an append-only ledger; expose read APIs. | Use case: Register Study Approval; Classes: LedgerEntry; State: Registration retries; Logic: chain registration step & fallback; Interface: Audit viewer. | Ledger adapter; Audit query UI. | Ledger append tests; tamper-evidence checks; node failure retries. |
| GOV-09 | IRB requirements include updated consent artifacts for digital/remote data collection and re-consent. | Version consent forms; require re-consent on material changes; maintain lineage to study versions. | Use case: Publish New Consent Version; Classes: StudyVersion, DynamicConsentForm; State: vN → vN+1; Logic: Sv → (Ia ∧ Pa); Interface: Version manager. | Versioning service; Consent renderer. | Traceability tests linking Sv to Ia/Pa; re-consent prompts triggered. |
| GOV-10 | Allocation of decision rights and accountabilities across actors is central to the framework. | Enforce segregation of duties; require dual approval (PI + IRB) before starting studies. | Use case: Start Study; Classes: DecisionRight, Approval; State: Ongoing gate; Logic: So → (Ia ∧ Pa); Interface: Start button gated by approvals. | Gatekeeper service; RBAC policies. | Negative tests: cannot start without both approvals. |
| GOV-11 | Ethics/privacy component directs how privacy rights must be protected; notification & acquisition must follow directives agreed by the committee. | Centralize privacy configurations; ensure notifications are policy-compliant and explainable. | Use case: Send Policy-aware Notification; Classes: Notification, Policy; State: Pending → Sent; Logic: consent prerequisites; Interface: Notification centre. | Privacy policy engine; Notification microservice. | Policy evaluation before send; audit of consents attached to notices. |
| GOV-12 | Framework is extensible: actors can be added/removed based on use case; self-directed transactions exist inside components. | Modular microservices and pluggable role definitions allow internal (component) workflows. | Use case: Add New Actor Type; Classes: Actor, Component; State: ActorRegistry update; Logic: transaction types; Interface: Admin console. | Service registry; RBAC config service. | Backward compatibility checks. |

| ID | Section 6 Governance Source | Derived Requirement (Section 7) | Design Artifact Mapping (Section 7) | Implementation Component (Consentio) | Verification/ Acceptance |
|---|---|---|---|---|---|
| GOV-13 | Need to address power imbalances and prepare for negotiations at nodal points. | Expose negotiation artifacts and history; support counter-offers for data access terms. | Use case: Negotiate Access Terms; Classes: Offer, CounterOffer; State: Draft ↔ Proposed ↔ Accepted; Logic: GAF negotiation; Interface: DSA negotiation UI. | Negotiation service; Commenting/attachment subsystem. | Traceable negotiation thread; acceptance recorded immutably. |
| GOV-14 | IRB/public entities require disclosure of IT infrastructure and DG practices; possible NDAs. | Support document management and role-limited access; capture attestations and NDA links in approvals. | Use case: Attach Compliance Docs; Classes: Document, Attestation; State: Verified; Logic: approval prerequisites; Interface: Compliance vault. | Document store; Attestation workflow. | Access controls validated; completeness checks before review. |
| GOV-15 | Framework insists on processes that are formal, stateful, and auditable across actors. | Define canonical state models for Study, Consent, DSA; enforce transition guards and record rationales. | Use case: Transition with Reason; Classes: TransitionLog; State: Guarded transitions; Logic: Spa → So (only if approvals); Interface: Reason capture modal. | Workflow engine; Reason logger. | Coverage that transitions require reasons; admin reports. |
| GOV-16 | Dynamic consent is central to empowering subjects and improving the acceptability of sharing. | Provide consent transparency (timeline, version diffs) and educational explainers about technology. | Use case: View Consent Timeline; Classes: ConsentHistory; State: N/A; Logic: display provenance; Interface: Timeline view + FAQs. | History API; Content service. | Users can see all changes; comprehension quiz passes thresholds. |
| GOV-17 | Distribution transactions include dissemination of knowledge/results per the rules from the authorities and IODG. | Allow publication of study outcomes to participants with policy-controlled timing and scope. | Use case: Publish Results to Participants; Classes: Result, Policy; State: Ready → Published; Logic: outcome visibility rules; Interface: Results page. | Results publisher; Policy gate. | Policy checks; participant access logs. |
| GOV-18 | Heterogeneous maturity among organizations; the platform must bridge gaps without compromising equity. | Offer APIs/adapters for varied data sources and maturity; default-secure, interoperable design. | Use case: Connect Data Source; Classes: Connector, Adapter; State: Connected; Logic: deny without consent/DSA; Interface: Source connectors. | Connector framework; Policy-enforced data ingress. | Integration tests against mock vendors; consent gates verified. |