

Doctoral Thesis

**A Multidisciplinary Approach to Governance
of Patient-Generated Health Data from
Mobile Health Wearables: Technical
Architecture, Standards, and Regulatory
Requirements**

by

Nuraini Muhammad Naim

Supervisor: Prof. Tomohiro Kuroda

Social Informatics Course

Graduate School of Informatics

Kyoto University

September 2025

A Multidisciplinary Approach to Governance of Patient-Generated Health Data from Mobile Health Wearables: Technical Architecture, Standards, and Regulatory Requirements

Abstract

The proliferation of consumer-grade wearable technologies such as smartwatches, fitness trackers, and smart rings has transformed how health data is generated, managed, and interpreted. These devices enable individuals to monitor physiological metrics continuously, giving rise to a new data category: patient-generated health data (PGHD). Unlike conventional clinical data collected within institutional healthcare settings, PGHD is created and managed outside formal systems through proprietary platforms operated by commercial technology providers. While PGHD holds significant promise for advancing personalised healthcare, preventive interventions, and AI-driven analytics, its governance remains underdeveloped, resulting in fragmented oversight, platform silos, limited data portability, and diminished user autonomy.

This thesis addresses the fundamental misalignment between governance structures and technical implementation in PGHD ecosystems. Rather than treating governance as an external constraint imposed after system design, effective frameworks must be embedded within the technical architecture itself. Adopting a multidisciplinary and design-oriented research approach, the study integrates legal analysis, policy review, and technical system design to explore how user rights, accountability, and interoperability can be operationalised in wearable health data infrastructures.

The core contribution is a governance-by-design framework that embeds user control, purpose limitation, consent management, auditability, and semantic standardisation directly into PGHD system architecture. This framework unifies policy, legal and technical components into a layered, implementable structure that supports governance principles across the entire data lifecycle, from edge devices to cloud storage and cross-platform analytics.

The study emphasises data standards and communication protocols as enablers of secure, interoperable, and rights-preserving data flows. While technical standards such as HL7 FHIR, OAuth 2.0, and User-Managed Access (UMA) offer useful functionalities for interoperability, consent management, and secure data exchange, their adoption remains uneven across platforms and jurisdictions. The primary governance challenge lies in selecting, aligning, and configuring these standards according to legal obligations, institutional mandates, and system-level goals. This thesis investigates how such standards can be selectively adapted and combined to support enforceable user rights within decentralised PGHD ecosystems, while exploring dynamic access control models that support context-aware permissions and evolving user preferences.

The framework draws on comparative analysis of digital health governance approaches in Malaysia, the European Union, and the United States, with additional insights from governance models in adjacent sectors, particularly open banking in financial services. These examples illustrate alternative regulatory logics, institutional configurations, and implementation strategies that inform the proposed architecture. A hypothetical use-case scenario demonstrates practical application, highlighting the integration of legal, policy, and technical components to support secure, rights-respecting, and innovation-enabling PGHD ecosystems.

By bridging the policy-technology divide, this study contributes theoretically and practically to the fields of health informatics, data governance, and regulatory design through an architecture-driven approach. The research demonstrates that by treating governance as a foundational design requirement rather than an external compliance constraint, digital health systems can simultaneously advance technological innovation and uphold user rights. This paradigm shift proposes digital services where user autonomy, data protection, and interoperability become intrinsic features of technical design rather than external requirements, offering practical guidance for policymakers, system architects, and platform providers seeking to develop ethical and scalable health data ecosystems.

Contents

Acknowledgement	vii
------------------------------	------------

List of Tables	x
-----------------------------	----------

List of Figures	xi
------------------------------	-----------

Introduction.....	1
--------------------------	----------

1.1	Background and motivation: Why this study matters	1
1.2	Problem statement: Misalignment between governance and technical realities.....	2
1.3	Framing the governance and architecture challenges: Key research questions.....	3
1.4	Research objectives	4
1.4.1	General objective.....	4
1.4.2	Specific objectives	4
1.5	Methodological approach and research strategies.....	4
1.6	Framing the challenges: Thesis structure	5
1.7	Research contributions: Societal impact and academic value	6
1.7.1	Academic contributions.....	6
1.7.2	Societal impact	6
1.7.3	Key deliverables	7

Literature review	8
2.1 Patient-Generated Health Data: A disruptive force in digital health.....	8
2.2 Technical foundations of Patient-Generated Health Data.....	9
2.3 Data governance concepts and models	10
2.3.1 Data governance: Definitional scope and working framework	10
2.3.2 Existing governance frameworks.....	12
2.3.3 Terminologies and definitions of data ownership.....	13
2.3.4 User agency: Consent and privacy principles	15
2.3.5 Accountability and enforcement mechanisms	16
2.4 Integrating Fragmented Literature: Justifying Research Approach	17
Methodology	18
3.1 Research philosophy and design	18
3.1.1 Research approach	18
3.1.2 Research strategy: Design-oriented framework development	19
3.1.3 Multi-domain integration approach	19
3.2 Research design and strategy	20
3.2.1 Overall research design.....	20
3.2.2 Case study approach.....	20
3.2.3 Multi-method integration	20
3.3 Data sources and collection.....	21
3.3.1 Primary data sources.....	21
3.3.2 Data selection criteria	22
3.3.3 Data collection strategy.....	22
3.4 Data analysis framework	23
3.4.1 Analytical approach	23
3.4.2 Analysis phases	23
3.4.3 Integration strategy.....	24
3.5 Quality assurance and validity	24
3.5.1 Ensuring research quality	24
3.5.2 Validity considerations	25

3.5.3	Reliability and transparency	25
3.6	Limitations and ethical considerations	26
3.6.1	Research limitations	26
3.6.2	Ethical considerations	26
3.6.3	Research integrity	27
3.7	Summary	27

Policy trajectories and the emerging digital health ecosystem in Malaysia.....29

4.1	Introduction	29
4.2	Navigating the public – private divergence: Digital health implementation in Malaysia’s healthcare system.....	29
4.3	Scope and framing of policy analysis	30
4.4	Policy evolution and comparative insights	32
4.4.1	Evolution of digital health policies in Malaysia	32
4.4.2	Exploring international digital health trajectories across selected countries	35
4.5	Sectoral divergence and innovation pathways.....	39
4.6	A growing presence of the digital health industry in the private healthcare sector in Malaysia	41
4.7	Regulatory gaps and governance challenges.....	42
4.8	Policy and practice implications	43
4.9	Conclusion	43

Governance Foundations: Legal, institutional, and policy context for wearable health data.....45

5.1	Introduction	45
5.2	Legal and regulatory landscape in Malaysia.....	46
5.2.1	Healthcare service regulations: Practitioners, facilities, pharmaceuticals and devices	46
5.2.2	Regulatory framework for personal data and digital health information	47
5.3	Digital health governance in Malaysia: Synthesis of institutional roles.....	51

5.3.1	Overview of Malaysia's digital health ecosystem	51
5.3.2	Key public institutions related to digital health governance ecosystem in Malaysia.....	52
5.3.3	Cross-sectoral and industry stakeholders.....	53
5.3.4	Coordination challenges and fragmentation.....	55
5.4	Global approaches to digital health data governance	55
5.4.1	European Union: Rights-driven, interoperable frameworks	56
5.4.2	United States: Innovation-led federated regulation	58
5.5	Thematic insights and applicability to Malaysia	62
5.5.1	Underlying limitations: Corporate control across jurisdictions.	62
5.5.2	Rights-based versus innovation-driven paradigms.....	65
5.5.3	Institutional coordination models	66
5.5.4	Applicability to Malaysia's dual healthcare system	67
5.5.5	Synthesis: Towards a hybrid model for Malaysia.....	67
5.6	Conclusion	69

Governance by design: Bridging principles and practice in the architecture of PGHD ecosystem70

6.1	Introduction	70
6.2	Technical standards landscape	71
6.2.1	Consumer health data platforms and technical frameworks	71
6.2.2	Interoperability challenges	73
6.2.3	Authorisation and access control standards	74
6.2.4	Security and privacy standards	77
6.2.5	Technical mechanisms for auditability and transparency.....	79
6.3	Access control in decentralised health systems.....	81
6.3.1	RBAC vs ABAC for PGHD environments.....	81
6.3.2	ABAC implementation and enforcement mechanisms	83
6.4	Cross-sector validation: Financial services model	86
6.4.1	Malaysian digital innovation and regulatory adaptation	86
6.4.2	Open banking as governance precedent	88
6.4.3	Technical architecture parallels	88

6.4.4	Standardised data exchange formats	89
6.4.5	Audit and transparency mechanisms.....	89
6.4.6	Governance framework effectiveness	90
6.4.7	Application to PGHD governance.....	90
6.5	Conclusion	92

Governance-by-design: A layered framework for PGHD systems ..94

7.1	Introduction	94
7.2	Legal obligations across the PGHD lifecycle	95
7.3	Governance-by-design: Embedding user autonomy in system architecture	96
7.3.1	Core principles and design philosophy	97
7.3.2	Governance principles to system design translation	98
7.3.3	Layered architecture for governance integration	99
7.4	Integrated data governance framework for PGHD	101
7.4.1.	Framework architecture and core domains.....	101
7.4.2.	Dynamic consent and authorisation mechanisms	102
7.4.3.	Cross-platform interoperability and semantic consistency	103
7.5	Governance principles integration with technical standards	103
7.5.1.	Legal framework alignment.....	103
7.5.2.	Technical standards synthesis.....	104
7.6	Framework validation through hypothetical scenario	105
7.6.1	Scenario walkthrough	105
7.6.2	Technical architecture validation	106
7.7	Conclusion	107

Discussion and contributions.....109

8.1.	Implementation challenges and governance integration	109
8.1.1	Device constraints and experience trade-offs	109
8.1.2	Semantic fragmentation and interoperability barriers	109
8.1.3	Security integration and Zero Trust Tensions	110

8.2.	Hybrid access control models	110
8.3.	Standardisation as a coordinating mechanism	110
8.4.	Contributions to theory and practice.....	110
Conclusion		112
Abbreviations.....		114
Bibliography.....		117

Acknowledgement

My path here has been anything but straightforward. I grew up in a family deeply rooted in mathematics, engineering and systems thinking, with my father directly involved in the country's early tech-forward agenda. Even when I was still in school, our family dinner conversations often revolved around technology and futuristic dreams. Computing and mathematics seemed to be the language spoken at home. Living in this world, I felt the need to take a different path to escape rivalry and carve out my own identity. I chose to study medicine, believing it would be a field far removed from theirs.

And yet, perhaps the pull was inevitable. Step by step, I found myself drawn back into the orbit of technology, not in the exact same path as my family but related, nonetheless. When I announced my decision to pursue a master's degree in health informatics, my brothers and sisters laughed and commented that their sister had finally returned to the rightful path. Through informatics, I found a way to bridge medicine with my unrealised ambition: law. What first felt like a detour has instead led me to a place where my different worlds finally converge. I now stand at the crossroads of disciplines, finding vocation in becoming a diplomatic interpreter between them.

Trust – a major theme in my work – has always been both my strength and my weakness. When I first arrived in Kyoto, I trusted that my years here would just be a simple break from the endless work responsibilities back home. Instead, I found myself tested in ways I never imagined. My grandmother passed away, my father required emergency surgery, and my children were missing me too much they began to rebel. There were moments when I wanted to abandon my research altogether, when the silence after hitting a brick wall felt heavier than the chaos I had left behind.

Against that backdrop, I am deeply grateful to my supervisor, Professor Tomohiro Kuroda, who, despite commenting after my first proposal presentation, *"I don't think you can graduate on time,"* continued to have faith in me. He quietly nudged me in the right direction whenever my ideas grew too scattered and provided an anchor to redirect me whenever I wandered off on a tangent. I am equally grateful to Professor Satoshi Yamada of the Graduate School of Law, Kyoto University, whose guidance as my external advisor was invaluable in shaping the legal dimension of this work and to

Professor Kei Hiroi of the Disaster Prevention Research Institute, Kyoto University, my internal advisor, for her never-ending support and encouragement.

I would also like to thank Professors Yukiko Mori, Yuki Kuroda, Goshiro Yamamoto, Chang Liu and Kazumasa Kishimoto for their patience in helping me to frame the thesis academically while navigating unfamiliar territory. Their support and encouragement pushed me forward when progress felt uncertain.

My gratitude extends to Roberto Espinoza Chamorro, Wataru Murata and Nattawipa Thawinwisan, whose steady progress during our weekly meetings pushed me to make progress in my own research instead of slacking off. I'm also thankful for their generous assistance in helping me prepare my thesis for submission, as well as the many shared plates of good food and countless cups of coffee. A special note of thanks goes to YuJu Liao, my little sister from another country who inspired me to become the older sister figure she could look up to and Saki Hirayama, whom I regarded as a sister even if she never realised it. My appreciation also goes to Thepphouthone Sorsavanh, whose solidarity as a fellow JICA scholar provided a sense of camaraderie throughout this journey.

I also wish to thank our lab secretaries, Ms. Yuko Furusawa and Ms. Yoko Hara, for their continuous patience and support, as well as Ms. Eriko Itoh from the International Student Division, whose kindness helped smooth many of the hurdles of the life of an international student in Japan.

This work was made possible through the support of the Japan International Cooperation Agency (JICA), whose sponsorship enabled me to pursue this doctoral degree while also immersing myself in Japanese culture through the community activities they regularly organised.

None of this would have been possible without the unfaltering support of my husband Muhammad Khairuzzaman Khairuddin, who for three long years took on the role of a single father to our two lovely children, AT-AT. I am so proud of my children for their perseverance in enduring life without their mother by their side. My utmost gratitude also goes to my parents, Naim Yunus and Sabariah Mohd Zin for their unwavering support of my studies, and to my brothers and sisters for being the loving uncles and aunts to my children. I am equally grateful to my parents-in-law, whose care and willingness to help look after the children eased many of the challenges of my absence.

To my Malaysian friends in Kyoto (and surrounding areas) who became my new family, thank you for cheering me on, for eating the food I cooked and for cooking for me. Thank you for laughing with me and for reminding me to stop when I laughed too much. To the Pom Pom Squad, thank you for your endless support and the good times we shared together. To the many others too numerous to name, thank you for the regular gossip that kept me updated on the happenings in Malaysia, and for the countless late-night memes that made the journey lighter.

Beyond individual names and groups, I am indebted to the broader academic and professional communities that shaped my thinking during these years. Conferences, seminars, and informal discussions with colleagues near and far reminded me that my work is part of a larger conversation on the future of digital health. These exchanges, even when brief, expanded my perspective and strengthened my conviction that governance must be built not only for systems, but for people.

I am also grateful to the networks and organisations that created spaces for dialogue across disciplines, where I could test ideas, learn from others, and gain the confidence to carry this research forward. These exchanges reminded me that research is never a solitary pursuit, but part of a continuous dialogue that transcends borders and disciplines.

Finally, I extend my thanks to my many sparring partners, both human and otherwise, whose relentless debates, challenges, and provocations sharpened my thinking and, in their own way, shaped this thesis into what it has become.

This thesis is more than an academic milestone. It is a testament to trust: in people, in ideas, and in the unexpected turns that carry us forward. Just as my research seeks to embed trust into the governance of patient-generated health data to empower individuals, I carry with me the trust of all who have walked beside me on this journey, embedded in my own, a source of guidance and empowerment as I move forward.

List of Tables

Table 1	Definitional approaches to data governance across orientations	11
Table 2	Conceptual distinctions between data ownership and custodianship in existing literature.	14
Table 3	Features of the healthcare systems studied	35
Table 4	Key Malaysian legal instruments relevant to healthcare service regulation	46
Table 5	Comparison of key heart rate data fields across different platforms (Google, Apple and Samsung)	73
Table 6	Technical component mappings between fintech and PGHD governance frameworks	91
Table 7	Legal and governance alignment across the PGHD lifecycle	95
Table 8	Translation of governance principles into technical architecture requirements	98
Table 9	Governance-aware system architecture: Layers, features, and regulatory alignment	100

List of Figures

Figure 1	Timeline of key milestones in Malaysia's national digitalisation agenda relevant to the healthcare sector.	34
Figure 2	Public and private healthcare expenditure, Malaysia (2009-2022)	40
Figure 3	Institutional and technological actors in Malaysia's healthcare ecosystem	52
Figure 4	Google Health Connect <code>HeartRateRecord</code> schema, including fields like <code>startTime</code> , <code>endTime</code> , <code>samples</code> , and <code>metadata</code> for heart rate data representation	71
Figure 5	Apple HealthKit <code>HKQuantitySample</code> schema used to represent heart rate measurements, including <code>quantity</code> , <code>startDate</code> , <code>endDate</code> and <code>metadata</code> .	72
Figure 6	Figure 6: Samsung Health SDK <code>HealthConstants.HeartRate</code> schema fields, including heart rate value, beat count, and metadata like timestamps and device UUID.	72
Figure 7	Timeline of financial services transformation in Malaysia.	87
Figure 8	Conceptual layered data architecture for mobile health wearables	96

Chapter 1

Introduction

1.1 Background and motivation: Why this study matters

The global health data landscape is undergoing a fundamental transformation. Consumer wearable technologies such as fitness trackers, smartwatches, and smart rings have evolved from simple step counters into sophisticated health monitoring systems that generate continuous streams of personal health data. The global wearable technology market, valued at USD 55.5 billion in 2022 is projected to reach USD 142.4 billion by 2030.⁽¹⁾ This reflects an unprecedented adoption of technologies that enable individuals to generate, monitor, and engage with their own health information outside traditional clinical settings. ⁽²⁾

This shift represents more than technological advancement. It signals a fundamental change in the nature of health data itself. Patient-generated health data (PGHD) emerges as individuals take control of their health monitoring, creating continuous, personalised datasets that exist independently of formal healthcare institutions. Unlike conventional health records produced within clinical settings under professional oversight, PGHD is generated by users themselves, often without direct healthcare provider involvement, creating new possibilities for preventive, personalised approaches to health management. ⁽²⁾

Yet this transformation has revealed a critical governance crisis. The ecosystem surrounding wearable health data involves a complex web of stakeholders such as device manufacturers, app developers, cloud service providers, analytics firms, and regulatory bodies, many of whom operate outside conventional healthcare regulation despite handling highly sensitive personal information. ^(3,4) Current governance frameworks, designed for institutional healthcare delivery, prove fundamentally inadequate for managing data that flows continuously across organisational boundaries, jurisdictions, and technical platforms.

The result is a profound misalignment between technological capability and governance reality. While wearable technologies promise to democratise health data

and empower individual health management, existing regulatory approaches often constrain rather than enable user autonomy. Users find themselves trapped within proprietary data silos, unable to meaningfully control how their self-generated health information is accessed, shared, or used. Valuable health data remains underutilised in fragmented systems rather than generating insights that could benefit both individual users and broader health innovation. (4)

This thesis argues that the solution lies not in more restrictive regulation, but in governance frameworks that enable genuine user control over health data while fostering innovation. Rather than treating governance as an external constraint on technical systems, effective frameworks must embed user rights directly into system architecture, making autonomy a natural consequence of technical design rather than a compliance afterthought.

The urgent need to resolve this governance-technology misalignment motivates this research, which explores how access control models, legal frameworks, and data architectures can be integrated to enable secure, ethical, and user-controlled data sharing in wearable health ecosystems.

1.2 Problem statement: Misalignment between governance and technical realities

Despite the widespread adoption of consumer wearables for personal health monitoring, their meaningful integration into healthcare delivery remains constrained by a fundamental misalignment between governance frameworks and technical implementation realities. Current regulatory approaches, designed for traditional clinical data systems, prove inadequate for governing PGHD that flows through complex, multi-stakeholder ecosystems involving device manufacturers, app developers, cloud services, and third-party analytics providers.

The core problem manifests in three interconnected ways:

- **Regulatory-technical disconnect**
Regulators lack deep understanding of data management protocols and technical infrastructures, while academic research on legal and governance mechanisms for emerging health data ecosystems remains underdeveloped. Existing frameworks treat governance as an external constraint on technical systems rather than embedding user rights directly into system architecture.
- **Innovation-governance paradox**
While the healthcare industry continues advancing consumer-driven digital health services, regulatory uncertainty creates a paradox where governance mechanisms intended to protect users and enable innovation end up constraining both. Companies hesitate to develop advanced analytics or data-sharing capabilities due to regulatory uncertainty, while users lack meaningful control over how their health data is accessed and used.

- Implementation fragmentation

The absence of semantic interoperability across wearable platforms prevents implementation of consistent governance mechanisms. When major health platforms employ incompatible data schemas even for universal metrics like heart rate, meaningful user control becomes technically impossible across the multi-vendor ecosystems that characterise real-world usage.

The fundamental issue is not insufficient regulation, but governance frameworks that constrain user autonomy rather than enabling it. Current approaches prioritise institutional control over individual agency, creating barriers to innovation while failing to deliver the user empowerment they purport to protect. This misalignment prevents realisation of wearables' potential as integrated healthcare tools and limits the development of user-centric digital health solutions.

1.3 Framing the governance and architecture challenges: Key research questions

This research addresses the governance-technology misalignment in wearable health data ecosystems through three interconnected inquiry domains:

Policy context and ecosystem development

1. How do national digitalisation policies and healthcare system structures influence the development of digital health ecosystems and PGHD innovation trajectories?
2. What lessons can be drawn from cross-sectoral governance approaches and international experiences to inform PGHD framework development?

Regulatory and governance frameworks

3. What are the key limitations in existing legal and institutional frameworks for governing PGHD, and how do these limitations constrain user autonomy and innovation?
4. How can governance principles such as user control, data portability, and accountability be operationalised within distributed wearable health ecosystems?

Technical architecture integration

5. How do current PGHD architectures handle data flows and access control, and where do they fail to support meaningful user autonomy?
6. How can technical architecture and governance mechanisms be integrated to enable secure, user-controlled data sharing that drives rather than constrains innovation in wearable health systems?

1.4 Research objectives

1.4.1 General objective

To develop user-centric governance frameworks for wearable health data that enable individual autonomy while fostering innovation, by integrating technical architecture with regulatory and policy mechanisms that embed user rights into system design.

1.4.2 Specific objectives

1. To assess legal and institutional frameworks against the requirements for user-controlled PGHD sharing, identifying how fragmentation and regulatory misalignment constrain individual agency.
2. To identify and analyse misalignments between governance frameworks and technical system design, particularly where legal and policy assumptions fail to reflect how data is generated, stored, and shared in wearable health ecosystems.
3. To develop architectural models that translate governance principles such as consent, user control, and auditability into enforceable technical mechanisms suitable for decentralised PGHD environments.
4. To design a layered governance framework that integrates legal, policy, and technical components, enabling secure, ethical, and interoperable data sharing across diverse platforms and stakeholders.

1.5 Methodological approach and research strategies

This study adopts an interdisciplinary approach that integrates health informatics, regulatory studies, and digital governance to address the complex sociotechnical challenges of wearable health data governance. Rather than treating technical architecture and governance as separate domains, the research develops governance-aware frameworks where user rights are embedded directly into technical system design.

The methodology combines document analysis, comparative case studies, and technical standards examination across three interconnected domains:

- Policy and ecosystem analysis
Understanding how national digitalisation strategies shape innovation and governance requirements, with focus on Malaysia and selected international comparisons.
- Regulatory and governance mapping
Identifying gaps and opportunities in current legal frameworks for enabling user-controlled data sharing.
- Technical architecture synthesis
Demonstrating how governance principles can be operationalised through system design rather than imposed through external regulation.

The methodological innovation lies in systematic integration across these domains to develop governance solutions that are technically feasible, legally coherent, and user-empowering. Cross-sector validation through financial services models provides evidence that user-controlled governance can drive rather than constrain innovation.

1.6 Framing the challenges: Thesis structure

This thesis is structured across eight chapters, progressing from problem framing and literature review to multi-domain analysis and the development of an integrated governance framework. The structure reflects the layered nature of the governance–technology misalignment and the need to examine policy, legal, and technical dimensions before proposing a governance-aware solution.

Chapter 1 introduces the research problem, outlines the study’s objectives and questions, and summarises the methodological approach. Chapter 2 reviews relevant literature, mapping existing debates and gaps across digital health governance, data access control, and technical standards. Chapter 3 outlines the interdisciplinary methodology used to integrate legal, policy, and technical analyses.

Chapter 4 situates the study within the broader policy and ecosystem context. It traces Malaysia’s digital health evolution and offers international comparisons to highlight structural enablers and limitations that shape the governance landscape. Although not directly tied to the research objectives, this chapter provides crucial contextual grounding for understanding the institutional and policy environment in which PGHD governance must operate.

Chapters 5 and 6 form the core analytical chapters. Chapter 5 examines the regulatory landscape, identifying legal and institutional misalignments that constrain user autonomy and governance effectiveness. Chapter 6 focuses on the technical domain, evaluating how current standards, architectures, and access control models address (or fail to address) user-centric governance requirements. This includes a cross-sectoral case study from financial data governance, which offers insight into how similar challenges structured consent and data interoperability have been addressed in another regulated ecosystem. These insights serve to highlight what is technically possible, and where current PGHD systems fall short.

Chapter 7 synthesises findings from the previous chapters into a governance-by-design framework. It presents a layered architecture that integrates legal, policy, and technical considerations, offering a design-oriented approach to embedding user rights, enforceability, and accountability in PGHD systems. A scenario walkthrough demonstrates how the framework could be applied in practice. Finally, Chapter 8 concludes with a discussion of the study’s key contributions, limitations, and implications for future research and policy reform.

1.7 Research contributions: Societal impact and academic value

This research contributes to digital health governance by proposing an integrated framework that bridges the persistent gap between technical capabilities and regulatory requirements in wearable health data ecosystems.

1.7.1 Academic contributions

- **Theoretical innovation**
The research introduces governance-aware architecture design as a novel approach where legal compliance and user rights are embedded directly into technical system architecture rather than imposed as external constraints. This challenges the conventional separation between governance and technical design in health informatics literature.
- **Methodological advancement**
Unlike existing literature that treats data architecture and governance as distinct domains, this thesis develops cross-domain integration methodology that systematically aligns technical standards with regulatory principles and user autonomy objectives.
- **Empirical validation**
The research provides the first systematic cross-sector validation of governance approaches between health and financial services, demonstrating that user-controlled data frameworks can accelerate rather than constrain innovation in sensitive data ecosystems.

1.7.2 Societal impact

- **Policy guidance**
The framework addresses a critical governance gap that has limited adoption of wearable health technologies, providing actionable recommendations for policymakers seeking to enable innovation while protecting user rights.
- **User empowerment**
By demonstrating how technical architecture can operationalise user autonomy, the research offers pathways for individuals to gain meaningful control over their health data rather than remaining dependent on institutional benevolence.
- **Innovation enablement**
The governance-by-design approach creates conditions for sustainable innovation by embedding user rights into system operation, reducing regulatory uncertainty while enhancing consumer trust.

1.7.3 Key deliverables

- Governance-aware data architecture framework for PGHD systems that embeds user control mechanisms into technical design.
- Cross-domain governance model that integrates policy, regulatory, and technical considerations into actionable implementation pathways.
- Evidence-based recommendations for enabling user autonomy while fostering innovation, validated through proven governance models from financial services.
- Implementation guidance for stakeholders across the digital health ecosystem, from policymakers and regulators to system developers and platform providers.

These contributions directly address the urgent need for governance frameworks that can operate effectively in the fragmented, multi-stakeholder environment that characterises contemporary digital health ecosystems.

Chapter 2

Literature review

2.1 Patient-Generated Health Data: A disruptive force in digital health

The healthcare sector is undergoing a profound transformation driven by advancements in digital technologies and the proliferation of mobile and sensor-based devices. (5,6) At the heart of this transformation lies the shift from traditional episodic models of care, where health data is collected intermittently within institutional settings to continuous, real-time monitoring enabled by personal health technologies. (7,8) This shift is an indication of a broader transition towards “Healthcare 4.0”, a term inspired by Industry 4.0 which reflects integration of connectivity, automation, data analytics and artificial intelligence into healthcare systems. (5)

One of the key changes in the new digital health ecosystem is the emergence of PGHD which is health-related data captured directly by individuals, often via consumer-grade wearable devices and paired with mobile phone applications. (2,9) Unlike conventional clinical data, PGHD is produced in non-institutional environments, under the control of users themselves, and often without direct mediation by healthcare systems. (9,10)

This decentralised mode of data production marks a fundamental shift in how health data is generated, validated and governed, prompting scholars to reassess traditional assumptions about data stewardship, clinical applications and regulatory oversight. (10) PGHD particularly challenges conventional notions of trust, accountability and regulatory scope in digital health ecosystems. (9,10)

As a result, PGHD is increasingly recognised as a distinct and disruptive class of health data, which calls for reconsideration of data ownership, management, consent and technical standards in non-traditional care environments. (2,9) As a disruptive data type operating outside traditional clinical boundaries, PGHD compels a rethinking of governance frameworks, technical standards, and regulatory logics that can no longer rely solely on institutional control and professional mediation as organising principles. (10)

This growing significance of PGHD is also reflected in policy initiatives such as the European Health Data Space and the U.S. 21st Century Cures Act, both of which aim to address data access, interoperability, and patient control in digital health systems. (11,12) These developments underscore the urgency of rethinking governance structures, which is explored further in subsequent sections.

2.2 Technical foundations of Patient-Generated Health Data

PGHD fundamentally differs from traditional clinical data in both its technical characteristics and the systems through which it is collected, processed, and shared. Generated outside institutional care settings, PGHD is produced continuously through wearable sensors, mobile applications, and connected devices, often without standardisation or oversight. This results in a class of health data that is heterogeneous in format, variable in granularity, and subject to vendor-specific design decisions. (9,13) Unlike electronic health records (EHRs), which are governed by clinical protocols and structured input systems, PGHD spans a spectrum of data formats. Some metrics such as heart rate, step counts and sleep stages are structured and machine-readable but are often stored in vendor-specific formats lacking standardised schemas or terminologies. Others, such as user-entered dietary logs or symptom journals are more variable or semi-structured, complicating interoperability and semantic alignment across systems. (13)

From a system architecture perspective, PGHD follows a markedly different data flow compared to institutional data systems. It is typically captured on a device, transmitted to a companion application, and uploaded to cloud infrastructure managed by the device manufacturer or affiliated service providers. Users often have limited visibility or control over how data flows beyond this primary ecosystem. These systems frequently operate outside formal healthcare infrastructures, resulting in challenges for integrating PGHD into electronic health records and established clinical workflows. The lack of interoperability and governance standards across device platforms further complicates consistent use within healthcare delivery. (14)

This decentralised data infrastructure introduces several access control and governance challenges. Traditional Role-Based Access Control (RBAC) models, designed for hierarchical, institutional environments, are poorly suited for ecosystems where users, third-party applications, and service providers may require varying levels of access to different types of data over time. More dynamic models, such as Attribute-Based Access Control (ABAC) and User-Managed Access (UMA), offer greater flexibility by incorporating contextual attributes such as data sensitivity, user intent, or third-party trust level. However, these models require technically mature infrastructure and granular metadata tagging, which are rarely supported across the commercial wearable health ecosystem. (9,15)

Moreover, interoperability remains a persistent obstacle. Although health data exchange standards such as HL7 FHIR and APIs like SMART on FHIR are

increasingly adopted in clinical contexts, they are inconsistently supported by consumer-grade devices and platforms. (16) Many device manufacturers rely on proprietary data schemas and closed platforms, restricting data portability and complicating integration into broader health information systems. (17) In practice, this limits not only clinical utility but also the feasibility of applying consistent governance and consent frameworks across platforms.

As a result, PGHD presents unique challenges that sit at the intersection of system architecture, data standards, and access governance. The technical decisions made at the device and platform level, often prioritising user experience, commercialisation, or analytics performance; have direct implications for what kinds of data rights, controls, and protections can be meaningfully enforced. Understanding these technical foundations is essential for designing governance frameworks that are not only legally sound but also implementable in the realities of digital health infrastructures. (9,10)

2.3 Data governance concepts and models

This section reviews key concepts underpinning data governance for PGHD in wearable ecosystems. It begins by examining the legal ambiguity surrounding data ownership, then considers how user agency is operationalised through consent and privacy principles. It further explores accountability and enforcement mechanisms and finally reviews broader governance models proposed for distributed data systems.

2.3.1 Data governance: Definitional scope and working framework

The concept of data governance lacks a universally accepted definition, with scholarly and practitioner communities applying the term across diverse contexts with varying emphases and scope. (18,19)

The absence of a universally accepted definition reflects data governance's inherently interdisciplinary nature, spanning legal frameworks, technical architectures, organisational policies, and ethical principles. However, this conceptual breadth has led to approaches that emphasise different priorities and deployment mechanisms when applied within the same data ecosystem.

In the context of consumer-generated PGHD, this lack of alignment complicates efforts to design cohesive governance strategies. To illustrate the landscape of fragmentation, this thesis categorises data governance approaches into four orientations, each reflecting different assumptions about where power resides, what governance seeks to achieve, and how it is operationalised. Table 1 illustrates example definitional approaches across these four orientations, highlighting how differences in emphasis result in governance models that are often ill-suited for cross-context application.

This typology serves as a foundational lens for the thesis's methodological focus, which deliberately concentrates on more structured and implementable aspects of governance, namely, technical standards and regulatory frameworks, rather than normative or organisationally contingent constructs such as data stewardship.

Table 1: Definitional approaches to data governance across orientations

Governance orientation	Core emphasis	Example literature	Governance priorities
Industry-oriented	Data quality, organisational control, compliance, accountability frameworks	Weber et al. (2009); Khatri & Brown (2010)	Centralised oversight, process standardisation, risk management, enterprise-wide accountability
System-oriented	Technical architecture, access control, interoperability, system integration, trustworthy AI	Janssen et al. (2020)	System integration, security protocols, performance optimisation, algorithmic accountability
Academic-oriented	Research integrity, reproducibility, ethical use, knowledge creation, open science	Wilkinson et al. (2016)	Research ethics, data sharing, reproducibility, FAIR principles, academic freedom
Public-oriented	Transparency, accountability, public value, democratic governance	Micheli et al. (2020)	Public accountability, transparency, citizen engagement, ethical AI governance

As Table 1 demonstrates, data governance has been conceptualised differently across various orientations, each emphasising particular aspects while often neglecting others.

Industry-oriented approaches typically focus on data quality, lifecycle management, and organisational compliance, treating individual rights as regulatory requirements rather than design principles. (20,21) These frameworks emphasise institutional control and operational efficiency, positioning data subjects as external stakeholders whose interests must be managed rather than empowered. Such approaches, while effective for enterprise contexts, fundamentally misalign with the distributed nature of consumer wearable ecosystems where no single entity maintains comprehensive control.

System-oriented literature defines data governance through technical and procedural lenses, emphasising access controls, audit mechanisms, interoperability standards, and algorithmic accountability. (22) While technically sophisticated, these frameworks often assume institutional contexts with clear hierarchies and stable stakeholder relationships. These assumptions do not hold in consumer wearable ecosystems where individuals interact with multiple autonomous entities across different jurisdictions. The focus on technical optimisation, while necessary, insufficiently addresses the power imbalances inherent in consumer-platform relationships.

Academic-oriented approaches emphasise research integrity, reproducibility, and knowledge creation through frameworks such as the FAIR principles (Findable, Accessible, Interoperable, Reusable). (23) While valuable for scientific contexts, these frameworks prioritise community benefit and open access over individual control, creating potential tensions with personal data sovereignty in health contexts.

Public-oriented scholarship approaches data governance through rights-based frameworks, emphasising privacy protection, democratic accountability, and public value creation. (19) However, these approaches often remain abstract regarding technical implementation, creating gaps between legal principles and operational realities in consumer technology contexts.

These definitional differences have practical consequences, as governance frameworks designed for one orientation often fail when applied to others, creating gaps in protection and accountability that are particularly evident in consumer health data ecosystems. The literature reveals a notable absence of frameworks that adequately address the distributed, multi-stakeholder nature of consumer wearable ecosystems, where individuals interact with multiple autonomous entities across different jurisdictions. This gap in the literature necessitates the development of new approaches that can bridge the identified orientations while addressing the specific challenges of personal health data governance in consumer technology contexts.

2.3.2 Existing governance frameworks

Several governance frameworks have been proposed or applied to digital health data, though none have yet achieved comprehensive adoption in consumer-grade PGHD environments. (24,25) The distributed nature of wearable health ecosystems, spanning multiple stakeholders, jurisdictions, and regulatory frameworks has prompted scholars to explore various approaches for managing data access, sharing, and accountability. (26)

Recent data governance frameworks have emphasised the need for managing complex, multi-stakeholder data environments, particularly in the context of AI and algorithmic decision-making systems. (24,25) These frameworks recognise that traditional centralised governance models are inadequate for ecosystems where data flows between autonomous entities with different policies, technical capabilities, and

regulatory obligations. (24) However, most distributed governance literature focuses on enterprise or research contexts rather than consumer-facing platforms, leaving significant gaps in addressing individual user rights and consent management. (26)

Big data governance frameworks have similarly attempted to address the complexity of managing large-scale, heterogeneous datasets. These approaches emphasise data quality, lifecycle management, and cross-organisational coordination, but often treat privacy and user consent as compliance requirements rather than fundamental design principles. The emphasis on organisational efficiency and analytics value extraction can conflict with user-centric governance principles essential for wearable health data. (25)

One of the more widely discussed models from research data management is the FAIR data principles (Findable, Accessible, Interoperable, and Reusable), introduced by Wilkinson et al in 2016. (23) While FAIR does not address governance or consent directly, it has informed interoperability frameworks that could support more structured data sharing in health ecosystems. However, the FAIR framework's focus on research data sharing may not adequately address the privacy, consent, and commercial considerations inherent in consumer wearable data ecosystems.

User-centric governance models have gained increasing attention as frameworks that prioritise individual agency and control over personal data. These models often advocate features such as consent dashboards, purpose-aware sharing, and fine-grained access controls that allow users to maintain ongoing oversight of how their data is used. While these ideas have been explored in the literature, especially in critiques of digital health rhetoric and the limits of user autonomy in data-driven systems, real-world implementation remains limited. (27) To date, most examples are either conceptual in nature or confined to tightly regulated clinical settings, with limited uptake in commercial wearable health ecosystems. (28)

This gap underscores the need for architecture-aware governance models, where consent, auditability, and policy enforcement are embedded into system design. This is a theme explored in the later chapters of this thesis.

2.3.3 Terminologies and definitions of data ownership

There is no standard or universally agreed-upon definition of data ownership in the context of PGHD. This ambiguity partly stems from the fact that legal frameworks typically avoid the term "ownership," opting instead for role-based classifications such as data controller, data processor, and data subject as defined in instruments like the GDPR and ISO/IEC 27701. (29–31) These classifications assign different levels of operational responsibility for how personal data is processed, but do not confer proprietary rights similar to traditional property ownership. (29,30) This distinction between data stewardship and data ownership becomes particularly important in

wearable health ecosystems, where multiple stakeholders may have different responsibilities for the same data.

Legal scholars have noted that wearables complicate traditional data controller-processor distinctions by creating ambiguity over control and responsibility. (32–34) Device manufacturers or app developers typically collect and store user data, technically acting as data controllers, while the individuals generating the data often have limited meaningful control over its subsequent use or dissemination. (32,35) This asymmetry has been identified as a fundamental governance concern in the literature, particularly when PGHD is used for purposes beyond those originally consented to or shared with entities not initially disclosed to users. (35,36)

Recognising these limitations, the literature has increasingly shifted toward data stewardship or custodianship models as alternative frameworks for governing personal data, particularly in health contexts. (37–39) Under stewardship models, entities that hold or manage data are positioned as trustees expected to act in the data subject's best interests, even while retaining technical or operational control over data processing. (23,38) These models are especially relevant for distributed ecosystems such as wearable health platforms, where users interact with multiple actors and services that may operate across different jurisdictions with varying regulatory frameworks. (38,40) The stewardship approach offers a more nuanced understanding of data relationships that moves beyond binary ownership concepts toward shared responsibility frameworks that can better accommodate the complex, multi-stakeholder nature of PGHD ecosystems. (39)

Table 2: Conceptual distinctions between data ownership and custodianship in existing literature.

Term	Core idea	Literature	Discussion
Data ownership	Legal or moral claim; or role-based control; often avoided in legal instruments	<i>Hummel et al (2021)</i>	Discusses philosophical tension and argues that “ownership” is not a stable legal category.
		<i>Purtova (2018)</i>	Argues that ownership doesn't fit with big data models and is not used in GDPR.
Data custodianship	Stewardship of data without legal ownership	<i>Rosenbaum (2010)</i>	Defines stewardship roles in health systems.
		<i>Hripcsak et al. (2014)</i>	Illustrates real-world custodianship in distributed health data networks.

Table 2 synthesises some of the key academic perspectives on data governance terminologies, highlighting how definitions vary and why consistent legal framing is difficult to establish.

While the literature frequently refers to concepts such as data ownership and custodianship, these terms lack consistent legal or technical definitions. “Ownership” is often used as a shorthand for control or rights over data, but it is largely avoided in legal frameworks such as the GDPR due to its conceptual and practical ambiguity. (29,30) “Custodianship” is commonly used in health policy discourse to denote institutional responsibility, yet it also lacks standard legal recognition. (37,38)

Given this ambiguity, this thesis avoids relying on the ownership/custodianship dichotomy as a primary analytical lens. Instead, it will focus on the terminology used in actual regulatory frameworks such as data controller, data processor, data user, and data recipient to ensure conceptual clarity and legal relevance in the analysis that follows, particularly in Chapter 5, where terminology from actual regulatory frameworks will be compared across jurisdictions.

2.3.4 User agency: Consent and privacy principles

Consent is widely acknowledged in the literature as a fundamental principle of data governance, yet empirical research has consistently demonstrated the inadequacy of current consent mechanisms in digital health platforms. (33,41) In the case of wearables, users typically provide one-time, blanket consent during account registration, often without meaningful understanding of downstream data uses. This practice falls far short of the informed consent standards required for meaningful privacy protection. (32,35) This model is increasingly recognised as fundamentally inadequate for PGHD, which is continuously collected and may be repurposed for secondary uses such as algorithmic analytics, targeted marketing, or commercial research without further user consultation.

More nuanced approaches have been proposed in the literature to address these limitations, including dynamic consent models that allow users to grant, revoke, or modify permissions over time and granular consent frameworks that enable purpose-specific authorisation. (39,42) However, these models remain largely theoretical, with limited practical implementation due to technical complexity and business model constraints. (43) Technical mechanisms such as OAuth 2.0 and User-Managed Access (UMA) provide frameworks for user-controlled access management. (44)

Privacy protection mechanisms in wearable ecosystems are often constrained by the proprietary nature of data flows and platform architectures. While privacy by design principles advocate for proactive privacy protection, the surveillance capitalism model demonstrates how digital platforms can exploit user data through opaque practices. (45,46)

International standards encourage the implementation of pseudonymisation and data minimisation, though empirical studies reveal inconsistent adoption across commercial platforms. (31,47,48) Furthermore, the literature identifies transparency challenges in how wearable devices handle health-related data sharing with third parties, with studies showing that data sharing agreements often lack transparency and adequate safeguards, creating information asymmetries that undermine users' ability to understand data practices. (49)

2.3.5 Accountability and enforcement mechanisms

The principle of purpose limitation which ensures that data is only used for the purposes for which it was originally collected is a foundational concept in data protection scholarship and is widely recognised in data governance frameworks globally. (29,31) However, the literature consistently identifies significant enforcement challenges in wearable ecosystems, where the distributed nature of data flows complicates traditional oversight mechanisms. Studies reveal that enforcement is weakened by vague terms of service, absence of metadata tagging, and limited oversight of third-party data recipients. (35,36)

Research demonstrates that users find it difficult to be confident that applications connected to their devices actually protect their personal data according to stated purposes, largely due to opaque data sharing practices and inadequate transparency reporting. (48) This challenge is compounded by the technical complexity of modern wearable ecosystems, where data may flow through multiple intermediaries before reaching its final destination, making it difficult to trace and verify compliance with original consent parameters.

Auditability emerges as another critical governance requirement in the literature, with scholars emphasising the need for comprehensive records of data access and usage to enable accountability and transparency. (38,40) However, empirical research reveals significant gaps in implementation across commercial wearable platforms. While audit trails are standard in regulated clinical systems, consumer wearables rarely offer users access logs or usage histories, undermining both regulatory oversight and individual accountability. (36,50)

Studies consistently show that commercial wearable platforms do not provide users with meaningful audit trails or access logs, with such features remaining primarily available in institutional or enterprise systems rather than consumer-facing applications. (48) This creates what scholars have termed an "accountability gap" where the technical capability for auditing exists but is not implemented in ways that serve user interests or regulatory oversight. (32,33) The absence of standardised auditability requirements for PGHD systems represents a fundamental governance challenge that undermines both individual agency and systemic accountability in wearable health ecosystems. (40)

2.4 Integrating Fragmented Literature: Justifying Research Approach

The preceding review reveals a persistent disconnect between technical literature on data architecture and access control, and the legal or policy-oriented research surrounding PGHD. While technical studies have proposed various enforcement models such as role-based access control (RBAC), attribute-based access control (ABAC), and token-based authentication, these approaches typically focus on system-level implementation without addressing how such mechanisms align with governance demands such as dynamic consent, individual control, or cross-border data portability. These technical discussions often overlook the sociotechnical realities of data sharing in consumer wearables, which involve diverse actors and data flows across platforms. (4,51)

Conversely, regulatory and policy literature has long emphasised the importance of protecting individual rights, ensuring accountability, and promoting ethical data use. Yet this body of work often remains abstract or normative, with little attention paid to how governance principles can be technically operationalised, particularly in decentralised, commercially driven health ecosystems where traditional regulatory safeguards may not apply and digital health services increasingly bypass conventional healthcare institutions altogether.

This fragmentation has resulted in critical gaps in both policy and design. Legal discussions highlight the importance of agency and control but offer limited strategies for enforcing these rights through architecture. Technical models prioritise system performance and data security but often fail to incorporate mechanisms that ensure legal compliance, user-facing transparency, or accountability for downstream data use.

This thesis addresses that gap by proposing a governance-aware framework that integrates legal and policy imperatives into technical system design. It does so by recognising that governance should not be treated as an afterthought or external constraint, but as a core architectural principle guiding data flows, access control, and stakeholder roles within the PGHD ecosystem.

This conceptual stance forms the basis for the research approach that follows, which integrates legal, policy, and technical analysis to examine how system architectures can better reflect governance priorities. The methodology outlined in Chapter 3 builds upon this foundation to design and evaluate a technical framework aligned with evolving digital health requirements.

Chapter 3

Methodology

Building on the conceptual foundations outlined in Chapter 2, this chapter details the research methodology used to develop and analyse the governance-aware framework.

3.1 Research philosophy and design

3.1.1 Research approach

This research addresses a practical problem on how to design governance frameworks that enable user control over health data while supporting innovation in digital health services. The study takes a problem-solving approach, focusing on developing practical solutions rather than testing theories.

Given the conceptual fragmentation of data governance outlined in Chapter 2, this study adopts a scoped focus on governance mechanisms that are technically operationalisable and legally enforceable. Specifically, the research emphasises formal regulatory frameworks (e.g., data protection laws) and technical standards (e.g., access control protocols), while excluding normative or organisational constructs such as data stewardship or civic data trusts. This decision ensures that the resulting governance framework is grounded in mechanisms that are feasible to implement within real-world wearable health data ecosystems.

This research recognises that governance frameworks and technical standards are designed systems which are not fixed but can be improved through systematic understanding and cross-sectoral insights. Rather than accepting existing arrangements as immutable, the study examines how they may be redesigned to better support data sharing, accountability, and end-user autonomy in the context of wearable health technologies.

The research philosophy emphasises practical, implementable outcomes over abstract theorisation. Knowledge is constructed by analysing how existing legal and

technical systems function in practice, identifying best practices from successful models and adapting them to the needs of patient-generated health data ecosystems.

3.1.2 Research strategy: Design-oriented framework development

This thesis adopts a design-oriented strategy, drawing from design science principles to create implementable governance frameworks for wearable health data. Rather than simply describing existing governance arrangements, the study seeks to reconfigure governance through structured integration of regulatory, technical, and institutional mechanisms. (52)

The approach is also emergent, where the analytical framework evolved iteratively during the research process. Insights from comparative legal analysis, technical standards, and institutional models were continually refined to shape a governance architecture that responds to the needs of decentralised, user-generated data environments. (53)

The research strategy involves:

- i. Analysis: Systematic examination of current governance approaches in Malaysia and internationally to understand strengths, weaknesses, and gaps.
- ii. Synthesis: Integration of insights from multiple domains (policy, law, and technology) to develop coherent and interoperable governance models.
- iii. Validation: Evaluating the proposed solutions against established frameworks in other regulated sectors (e.g., financial services) and applying them to a hypothetical data-sharing scenario to assess feasibility, scalability, and robustness.

3.1.3 Multi-domain integration approach

The research integrates analysis across three key domains to inform the development of governance frameworks:

- i. Policy context: How national digitalisation strategies and healthcare policies create opportunities and constraints for governance innovation.
- ii. Governance frameworks: How legal and regulatory structures affect user control and innovation, and where gaps exist.
- iii. Technical implementation: How governance principles can be built into technical systems rather than imposed from outside.

By examining all three areas together, the research develops governance solutions that are practical, legally sound, and technically feasible.

3.2 Research design and strategy

3.2.1 Overall research design

This research employs a qualitative, design-oriented approach combining legal, policy, and technical analysis to develop and validate a governance framework for patient-generated health data. The study combines document analysis, comparative case studies, and technical standards examination to build comprehensive understanding across policy, regulatory, and technical domains.

The research design is structured around framework development rather than hypothesis testing. Instead of starting with predetermined theories to test, the study builds new conceptual frameworks by systematically analysing existing approaches, identifying gaps and opportunities, and synthesising insights into actionable recommendations. The design deliberately concentrates on formal mechanisms that are enforceable and implementable, such as legal provisions, data management standards, and organisational protocols. This avoids reliance on abstract or normative concepts like data stewardship and ensures that the resulting framework addresses governance as a system that can be practically embedded within real-world infrastructures.

3.2.2 Case study approach

The research uses Malaysia as the primary case with international comparisons to provide context and validation. (54) This approach enables:

- Deep contextual understanding: Malaysia's dual public-private healthcare system and active digitalisation agenda provide rich insights into governance challenges facing middle-income countries.
- Comparative learning: Analysis of EU and US approaches offers contrasting models of how governance can be structured, while examination of countries like Estonia and Denmark provides examples of successful implementation.
- Cross-sector validation: Malaysia's experience with fintech innovation and regulatory sandboxes provides real-world evidence that user-controlled governance can drive innovation while maintaining appropriate protections.

3.2.3 Multi-method integration

The study combines several analytical methods:

- Document analysis: Systematic review of policy documents, legal frameworks, technical standards, and academic literature to understand current approaches and identify gaps. (55)
- Comparative analysis: Structured comparison across jurisdictions and sectors to identify successful governance models and assess their transferability.

- Technical standards analysis: Detailed examination of data management protocols and access control mechanisms to assess what governance approaches are technically feasible.
- Framework synthesis: Integration of findings across all methods to develop new governance approaches that are practical, legally sound, and technically implementable.

This multi-method approach ensures that the resulting governance framework is grounded in evidence from multiple sources and perspectives.

3.3 Data sources and collection

3.3.1 Primary data sources

The research draws on four main categories of data sources to ensure comprehensive coverage across policy, regulatory, and technical domains:

Policy and Planning Documents

- Malaysia Plans (Fifth through Twelfth, 1986-2025) providing chronological analysis of digital health policy evolution
- National strategies including Digital Economy Blueprint, National AI Roadmap, and Ministry of Health digitalisation plans
- Sectoral policies and implementation guidelines from relevant ministries and agencies

Legal and Regulatory Frameworks

- Malaysian legislation including Personal Data Protection Act, Data Sharing Act 2025, and healthcare service regulations
- International frameworks including EU GDPR, European Health Data Space, US 21st Century Cures Act, and HIPAA
- Regulatory guidance documents and implementation studies from various jurisdictions

Technical Standards and Specifications

- Data management standards including OAuth 2.0, User-Managed Access (UMA), and HL7 FHIR
- Platform documentation from major health data ecosystems (Google Health Connect, Apple HealthKit, Samsung Health)
- Security and privacy standards including ISO/IEC 27000 series and NIST guidelines

Academic and Industry Literature

- Peer-reviewed publications on digital health governance, access control, and health informatics
- Industry reports and white papers from technology companies and consulting firms
- Policy analysis and recommendations from international organisations and think tanks

3.3.2 Data selection criteria

Relevance: Documents must directly address governance of personal health data, digital health policy, or technical standards for health data management.

Authority: Sources include official government publications, established technical standards bodies, peer-reviewed academic journals, and recognised industry organisations.

Currency: Primary focus on materials from 2016-2025 for contemporary relevance, with historical documents from 1986-2015 included for policy evolution analysis.

Accessibility: All sources are publicly available documents, ensuring transparency and enabling verification of findings.

Language: Documents in English and Bahasa Malaysia, with official translations used where available for Malaysian government materials.

3.3.3 Data collection strategy

Systematic search: Structured searches of government databases, academic databases, and technical standards repositories using predetermined keywords and search terms.

Snowball sampling: Following references and citations from key documents to identify additional relevant sources and ensure comprehensive coverage.

Expert recommendations: Incorporating key documents identified through the author's professional networks and academic supervisory guidance.

Currency updates: Regular monitoring of policy announcements and technical standard updates throughout the research period to capture recent developments.

3.4 Data analysis framework

3.4.1 Analytical approach

The framework development process involved iterative synthesis of insights from the three domains outlined earlier. Rather than imposing a theoretical structure from the outset, the framework emerged through engagement with legal texts, technical standards, and comparative models. The process was guided by the goal of developing a governance framework that is practically feasible, enforceable, and operationalisable across technical and institutional settings.

In line with the thesis scope, the framework emphasises mechanisms that can be embedded into regulatory systems, technical architectures, or institutional workflows, avoiding constructs that rely on voluntary adoption or normative roles alone. This ensures the proposed model supports actionable governance that can be realised within real-world PGHD ecosystems.

3.4.2 Analysis phases

Phase 1: Familiarisation and initial coding

- Comprehensive reading of all source materials to develop overall understanding of the governance landscape.
- Initial identification of key themes, concepts, and stakeholder roles across different domains.
- Development of preliminary coding framework based on research questions and emerging patterns.

Phase 2: Systematic coding and pattern identification

- Application of coding framework across all documents using qualitative analysis principles.
- Identification of recurring themes, contradictions, and gaps within and across domains.
- Development of thematic matrices organising findings by domain, jurisdiction, and governance principle.

Phase 3: Comparative analysis

- Structured comparison of governance approaches across jurisdictions (Malaysia, EU, US, selected countries).
- Cross-sector analysis comparing health governance with financial services models.
- Temporal analysis tracking policy evolution and implementation outcomes.

Phase 4: Gap analysis and synthesis

- Systematic identification of misalignments between governance frameworks and technical requirements.
- Analysis of institutional coordination challenges and accountability gaps.
- Integration of findings to identify opportunities for governance innovation.

Phase 5: Framework development

- Synthesis of insights into coherent governance principles and implementation mechanisms.
- Development of architectural recommendations that operationalise governance through technical design.
- Creation of actionable recommendations for different stakeholder groups.

3.4.3 Integration strategy

The analysis culminates in cross-domain synthesis that integrates findings across the three main analytical areas:

- Policy context to technical requirements: Understanding how national digitalisation strategies and healthcare system structures create specific governance needs that must be addressed through technical implementation.
- Regulatory gaps to architecture solutions: Mapping existing legal frameworks against technical capabilities to identify where governance principles can be operationalised through system design rather than external regulation alone.
- Cross-sector validation to implementation pathways: Using proven governance models from financial services to validate the feasibility of proposed approaches and develop practical implementation strategies for health data governance.

This integration strategy ensures that the final governance framework bridges policy intentions, regulatory requirements, and technical possibilities into actionable recommendations for stakeholders across the digital health ecosystem.

3.5 Quality assurance and validity

3.5.1 Ensuring research quality

Comprehensive coverage: The research ensures quality through systematic inclusion of diverse source types across policy, regulatory, and technical domains. This multi-source approach reduces the risk of bias from any single category of documents or perspectives.

Source triangulation: Findings are validated by comparing insights across different types of sources (government documents, technical standards, academic literature, industry reports) to ensure consistency and identify areas of convergence or disagreement.

Temporal validation: The longitudinal analysis of policy evolution from 1986-2025 provides confidence in identified trends and patterns, enabling distinction between temporary policy shifts and sustained directional changes.

Cross-jurisdictional verification: Comparative analysis across multiple countries and regions helps verify that identified governance challenges and solutions are not unique to specific national contexts.

3.5.2 Validity considerations

Content validity: The research addresses validity through comprehensive coverage of relevant governance domains and systematic inclusion of authoritative sources from government, industry, and academic contexts.

Construct validity: Key concepts (user autonomy, governance-aware architecture, semantic interoperability) are clearly defined and consistently applied throughout the analysis, with operational definitions grounded in existing literature and technical standards.

External validity: Malaysia's characteristics as an upper middle-income country with mixed healthcare systems and active digitalisation initiatives enable insights transferable to similar contexts globally, while international comparisons strengthen generalisability.

3.5.3 Reliability and transparency

Systematic documentation: All sources are comprehensively cited, and analytical procedures are clearly specified, enabling verification and replication of the research approach.

Analytical transparency: The coding framework, thematic development process, and synthesis procedures are explicitly described, allowing assessment of analytical rigor and consistency.

Reflexivity: The author's professional background in Malaysian public health governance is acknowledged as both an analytical asset (providing institutional understanding) and potential source of bias (requiring validation through international comparison and cross-sector analysis).

3.6 Limitations and ethical considerations

3.6.1 Research limitations

- **Conceptual vs. empirical approach**
This research develops governance frameworks through document analysis and comparative study rather than empirical testing with real users or systems. While this approach enables comprehensive framework development, it limits claims about real-world effectiveness until the frameworks are implemented and evaluated in practice.
- **Geographic focus**
The primary case study focuses on Malaysia, which may limit generalisability to countries with different healthcare systems, regulatory traditions, or levels of digital development. However, international comparisons and cross-sector validation help address this limitation.
- **Stakeholder representation**
The research relies on document analysis rather than direct consultation with key stakeholders including patients, healthcare providers, technology companies, and regulators. Future research incorporating stakeholder perspectives would strengthen the practical applicability of the proposed frameworks.
- **Technical implementation detail**
While the research identifies technical standards and approaches that can support governance objectives, it does not provide detailed implementation specifications for specific platforms or contexts. Such specifications would require additional technical development and testing.
- **Temporal currency**
The rapid evolution of both technology and regulation means that specific technical recommendations may require updating as platforms, standards, and legal frameworks continue to develop

3.6.2 Ethical considerations

- **Public document analysis**
This research analyses publicly available documents and frameworks, avoiding direct involvement of human subjects. However, the governance implications of the research require consideration of broader ethical issues.
- **Privacy and autonomy**
The research advocates for increased user control over health data, which aligns with principles of individual autonomy while requiring careful balance with appropriate privacy protections.
- **Equity and access**

The proposed governance frameworks are designed to avoid creating barriers for vulnerable populations or exacerbating digital divides, though implementation would require ongoing monitoring to ensure equitable outcomes.

- Innovation and safety

The research seeks to enable innovation while maintaining appropriate safeguards, recognising the need to balance technological advancement with patient safety and data protection.

3.6.3 Research integrity

- Transparency

All sources and analytical procedures are fully documented, enabling verification and assessment of the research approach and findings.

- Bias acknowledgment

The author's professional background and philosophical commitments to user autonomy are explicitly acknowledged, with mitigation strategies including international comparison and cross-sector validation.

- Objective analysis

Despite advocating for user-centric governance, the analysis strives to fairly represent different governance approaches and their trade-offs rather than selectively presenting only supporting evidence.

3.7 Summary

This methodology chapter has outlined a comprehensive approach to developing governance frameworks for patient-generated health data that bridges policy analysis, regulatory review, and technical implementation. The research design combines document analysis, comparative case studies, and technical standards examination to create actionable recommendations that are simultaneously policy-informed, legally coherent, and technically feasible.

The multi-domain analytical approach enables the research to address the fundamental challenge identified in Chapter 1 on the misalignment between governance frameworks and technical realities in digital health ecosystems. By systematically analysing policy evolution, regulatory gaps, and technical capabilities, the methodology provides a solid foundation for developing governance-aware architectures that embed user rights into system design.

The use of Malaysia as the primary case, supported by international comparisons and cross-sector validation, ensures that the resulting frameworks are both contextually grounded and broadly applicable. The cross-sector validation through financial

services governance models provides empirical evidence that user-controlled data governance can drive innovation while maintaining appropriate protections.

The limitations acknowledged in this chapter, particularly the conceptual rather than empirical nature of the approach, point toward important directions for future research, including stakeholder consultation, pilot implementation, and real-world testing of the proposed frameworks. However, the methodology as designed provides the necessary analytical foundation for developing the comprehensive governance framework presented in Chapter 7.

The analytical framework established here directly supports the thesis objectives by ensuring that the final governance recommendations are grounded in systematic analysis across all relevant domains rather than theoretical speculation. This methodological rigor is essential for producing frameworks that can guide practical implementation by policymakers, regulators, and system developers.

Chapter 4

Policy trajectories and the emerging digital health ecosystem in Malaysia

4.1 Introduction

While digital health is gaining global traction, the readiness of national ecosystems to support innovation varies widely. Malaysia's digital health ecosystem has evolved within a broader national digitalisation agenda that embraces innovation, cross-sector experimentation, and societal openness to emerging technologies.

This chapter explores the trajectory of Malaysia's digital health policy over the past four decades, highlighting key enablers such as strategic policies, infrastructure investment and regulatory sandboxes which have supported the growth of innovation while also underscoring the divide between the public and private healthcare sectors.

4.2 Navigating the public – private divergence: Digital health implementation in Malaysia's healthcare system

Malaysia's healthcare system, characterised by its dual public-private structure, has undergone significant transformation since the 1980s. While digital health initiatives were introduced relatively early compared to global trends, the implementation and adoption rates have varied significantly between the public and private sectors.

Malaysia, classified as an upper middle-income country by the World Bank Group, operates its public healthcare sector through the Ministry of Health (MoH), funded by general taxation, providing universal access at nominal charges to all Malaysians regardless of income, with free services for maternal and child health as well as infectious diseases. The private sector, in contrast, operates on funding through out-of-pocket payments, private insurance, or insurance coverage provided by private corporations to their employees. (56) This dual system creates distinct pathways for digital health implementation and adoption.

The scale and scope of these two sectors are significantly different. As of December 2022, the public sector operates 148 hospitals and special medical institutions (45,167 beds) and over 3,000 clinics, while the private sector comprises 207 hospitals (17,781 beds) and 9,830 registered medical clinics. Public facilities handle most of the healthcare utilisation, with MoH institutions accounting for 69.23% of total hospital admissions and 74% of outpatient attendance in the hospitals. (57) While a total of 39,141,568 attendances were recorded at the MoH primary care facilities, no comparative data is available for the attendance at the general private clinics. (57)

Healthcare financing in Malaysia reflects this dual structure. In 2021, total health expenditure reached RM78.22 billion (5.06% of GDP), with the public sector accounting for 57.85% of this expenditure, 49.33% of which was by the MoH. (2, 3) Out-of-pocket payments (OOP) represent the second-largest source of financing at 31.51%. (58) Despite high OOP rates, Malaysia maintains relatively low catastrophic healthcare expenditure at 2.8%, compared to the global estimate of 11.7%, suggesting effective financial protection mechanisms. (59) The National Health Accounts report indicates that OOP spending primarily covers outpatient services (40.5%), inpatient services (24.6%), and “health education and training” (6.0%). (58)

The private healthcare sector shows distinct characteristics in terms of distribution and digital readiness. Private facilities are predominantly concentrated in urban areas, influenced by factors such as education levels, health awareness, and financial capabilities. (60,61)

Recent studies indicate growing digital health engagement among urban populations, with a PricewaterhouseCoopers survey in Klang Valley reporting that 63% of respondents invest in physical and mental wellbeing, while 45% use health monitoring devices or apps. 45% of respondents also self-diagnose symptoms and treatments online prior to seeking consultation. (62)

This unique healthcare landscape presents both opportunities and challenges for advancing digital health initiatives. The willingness of Malaysians to pay for healthcare services, particularly in health education and training, coupled with increasing digital health adoption in urban areas, suggests potential for growth in digital health initiatives. However, the dual system structure necessitates careful consideration of how digitalisation policies can be effectively implemented across both public and private sectors while maintaining equity in healthcare access and quality.

4.3 Scope and framing of policy analysis

This chapter examines the evolution of Malaysia’s healthcare digitalisation policies from 1986 to 2025 and their influence on the development of digital health across the country’s dual-sector system. Expanding upon the research framing in Chapter 1 and the methodology described in Chapter 3, this analysis focuses on how strategic

planning, infrastructure investment, and governance priorities have shaped Malaysia's digital health landscape.

The chapter draws on a narrative review of national planning and policy documents, supported by illustrative comparisons with selected high-income countries, including Sweden, Denmark, the United Kingdom, and Estonia. Particular attention is given to identifying structural enablers and constraints in both public and private sectors, which have followed diverging trajectories in digital health adoption. Tracing these developments offers policy-relevant insights into how innovation emerges within institutional and governance contexts.

The analysis synthesises three primary categories of documents:

1. Official government documents: including the Fifth through Twelfth Malaysia Plans, Ministry of Health strategies, and national digitalisation policy documents.
2. Statistical and technical data: including reports from the Ministry of Health and international health indicators from the World Bank.
3. Supporting literature: including peer-reviewed publications, industry reports, and verified media sources—particularly where academic literature is sparse, such as in the private healthcare sector.

Documents were reviewed in both Bahasa Malaysia and English to ensure comprehensiveness, with official translations used where available. Media sources were selectively included to provide contextual updates on recent developments in policy and innovation.

The analytical process was iterative and theme-driven, allowing for emergent connections that may have been missed in a more rigid structure. The review is organised around three complementary analytical perspectives:

- **Chronological Analysis:** Malaysia's five-year development plans were analysed to trace the evolution of digital health strategies, identify turning points, and assess implementation outcomes. Cross-referencing with referenced policies and follow-up documents provided deeper insights into success factors and policy discontinuities.
- **International Context:** To situate Malaysia's trajectory globally, exploratory comparisons were made with four countries that reflect a range of digital health adoption models. Sweden and Denmark represent early adopters with integrated national systems; the UK offers institutional and historical parallels with Malaysia; and Estonia serves as a global benchmark in digital health transformation. Key macro indicators (e.g., GDP, health expenditure, life expectancy, population density, physician ratios) were drawn from World Bank datasets to contextualise system-level capacities. Base reference documents include UN and EU eHealth strategy briefs.

- **Systems Thinking Perspective:** A systems thinking lens was applied to examine how public and private sector developments have evolved in parallel, often with limited integration. This perspective highlights how government interventions affect various stakeholders differently across institutional boundaries and sheds light on the structural fragmentation of the healthcare ecosystem.

While the analytical framework offers a flexible and comprehensive lens, it is important to acknowledge several limitations that may shape the scope and interpretation of the findings. The selection of comparator countries was based on subjective criteria, including perceived digital maturity and the availability of English-language sources. Additionally, the grey literature may have omitted internal government drafts, policy updates, or studies not available in public databases. As a narrative review, the interpretation of policy themes and inflection points carries inherent subjectivity, and the depth of analysis varies depending on the availability of source materials across different time periods.

4.4 Policy evolution and comparative insights

4.4.1 Evolution of digital health policies in Malaysia

Strategic development plans have guided Malaysia's national development since prior to gaining independence in 1957. The Fifth Malaysia Plan (1986-1990) marked a significant shift towards infrastructure development, particularly in telecommunications and utilities as heavy industrialisation and privatisation became key strategies for economic development. (63) The Seventh Malaysia Plan (1996-2000) saw a major focus being placed on information and communication technology (ICT) development agenda. (63) The subsequent Malaysia Plans had evolved to incorporate ICT as key enablers in economic activities in various sectors before becoming a targeted economic activity by itself.

A similar trajectory can be observed in the healthcare sector. The earlier Malaysia Plans were only focused on improving and expanding basic healthcare services through public healthcare facilities to improve population health outcomes. Subsequently it began to incorporate digitalisation initiatives before eventually recognising the private healthcare industry and digital health services as an economic contributor.

The early computerisation phase began under the Fifth Malaysia Plan (1986-1990) with the introduction of computerised billing systems in selected government hospitals. (64) The Sixth Malaysia Plan (1991-1995) expanded this administrative computerisation, implementing systems for quality assurance and budget performance monitoring. (64,65)

Under the Seventh Malaysia Plan (1996-2000), Malaysia launched a nationwide ICT agenda to support the sector and its related industries. This period saw several landmark developments including the establishment of the Multimedia Super Corridor,

enactment of the Telemedicine Act 1997, and release of the comprehensive Telemedicine Blueprint. (66,67) The Blueprint outlined several ambitious projects such as the “Mass Customised/Personalised Health Information and Education” project, the “Continuing Medical Education” (CME) project, teleconsultation services, and the “Lifetime Health Plan” project. (67) This era also witnessed the establishment of Malaysia’s first paperless hospital with the implementation of Total Hospital Information System (THIS) at Hospital Selayang in 1999, followed by Hospital Putrajaya in 2000, both of which were MoH hospitals. (68)

However, the Asian Financial Crisis caused Malaysia Plans to shift into more short- and medium-term issues related to economic stabilisation rather than long term plans for growth, reflecting the nation’s priority on economic recovery. (63) While various plans continued to take place to position Malaysia as a major global ICT hub under the Eight Malaysia Plan (2001-2005), healthcare digitalisation was noticeably absent from the healthcare services section of the document. (69)

The Ninth Malaysia Plan (2006-2010) emphasised macroeconomic stability and positioned ICT as a driver for new sources of growth and enhanced productivity and competitiveness. (70) This was reflected in the National Strategic ICT Roadmap which highlighted three technology focus areas: wireless sensor networks, predictive analytics, and 3-dimensional internet. (71) The National Health Informatics Centre was established under the Ministry of Health to centralise health and health-related data management at the federal level. However, no new Hospital Information System (HIS) projects were announced during this period while medical tourism began to emerge as a new economic sector. (70)

The Tenth Malaysia Plan (2011-2015) streamlined the role of the government as a regulator and catalyst while upholding effective delivery of services. While ICT was identified as one of the 12 National Key Economic Areas (NKEA) identified under this plan, the public healthcare sector was more focused on services expansion rather than digitalisation agenda. At the same time, the private healthcare sector was introduced as one of the NKEA. (72)

The Eleventh Malaysia Plan (2016-2020) emphasised ICT infrastructure and talent development as key enablers for economic growth. (73) The Malaysian Health Data Warehouse (MyHDW), conceptualised in 2011, was finally launched in 2018, integrating data from various government agencies as well as both public and private healthcare facilities. (74,75) MyHDW was established with the aim to facilitate disease surveillance and research activities, thus allowing better evidence-based health system management. (76) This system’s successful integration with Geographic Information System (GIS) proved to be a useful tool for an effective control of the COVID-19 pandemic in 2020. (77)

The Twelfth Malaysia Plan (2021-2025) was prepared with post-pandemic economic recovery in mind. It marked a significant push towards digital transformation which would serve as an important enabler across three key themes: resetting the economy;

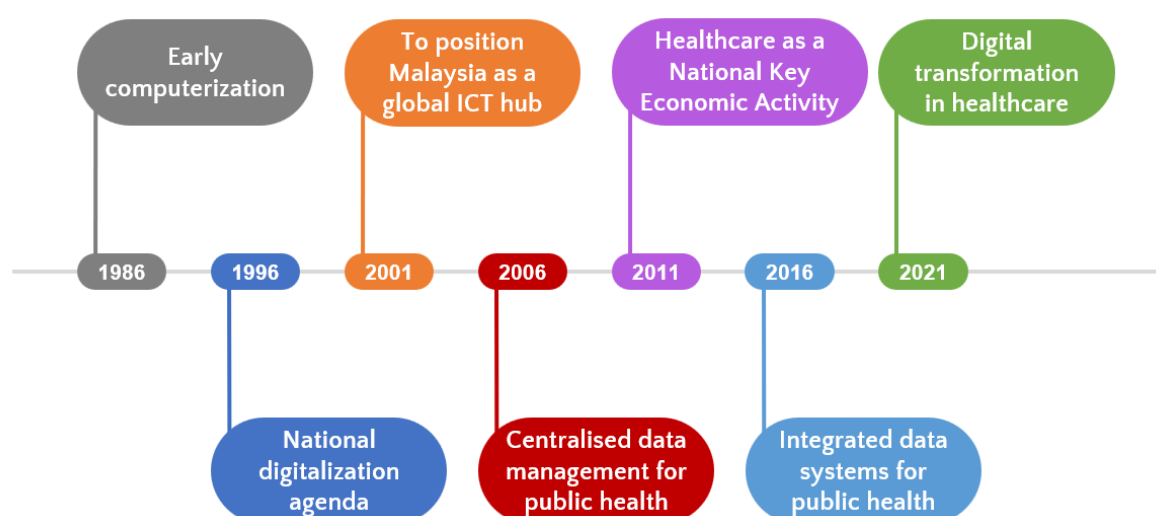
strengthening security, wellbeing and inclusivity; and advancing sustainability. The plan integrates several initiatives such as the National Fourth Industrial Revolution (4IR) Policy, Digital Economy Blueprint and National e-Commerce Strategic Roadmap 2.0. The National Internet of Things (IoT) Strategic Roadmap will also be reinvigorated. (78)

In the healthcare sector, the plan focuses on health system reform and services redesign. Key digital health initiatives include the revival of lifetime health record, which was first proposed in the 1997 Telemedicine Blueprint, expansion of virtual clinic services, development of mobile application for appointment and medical record access and implementation of e-hailing home-based healthcare services. The plan also addresses Malaysia's ageing population through IoT-enabled homecare monitoring and virtual consultations. (78)

MyHDW would be enhanced with a virtual platform to facilitate cross-agency data sharing, and the National Institutes of Health (NIH) will have a new digital health research centre. (78) This is further supported by the Ministry of Health's digitalisation strategic plan which outlines four strategic thrusts, thirteen strategies and thirty digitalisation programmes to be implemented throughout the ministry and its healthcare facilities. The plan highlights the aim to establish robust end-to-end digital health services by adapting emerging 4IR technologies. (79)

Figure 1 highlights major national initiatives from the Fifth Malaysia Plan (1986-1990) through the Twelfth Malaysia Plan (2021-2025) that have shaped Malaysia's digital transformation, with a particular attention to milestones relevant to the healthcare sector.

Figure 1: Timeline of key milestones in Malaysia's national digitalisation agenda relevant to the healthcare sector.



While Malaysia's digital health journey reflects a gradual evolution shaped by national policies and domestic situations, international experiences offer valuable reference points for understanding what alternative trajectories might look like. The next section explores how four countries have structured their digitalisation efforts in ways that reveal both parallels and contrasts with Malaysia's approach.

4.4.2 Exploring international digital health trajectories across selected countries

Sweden and Denmark were chosen because they were early adopters to a national digitalisation agenda. The United Kingdom was chosen due to its historical influence and similarities with the Malaysian healthcare system while Estonia was selected as it is generally considered a pioneer in digital health. All these countries have a similar funding model to Malaysia except for Estonia as the public funding is generated through an insurance system. Compared to all these countries, Malaysia has the lowest healthcare expenditure (% to GDP) and doctor to population ratio. Table 3 summarises the key features of the countries compared in this study (56,80–88).

Table 3: Features of the healthcare systems studied

	Malaysia	Sweden	Denmark	United Kingdom	Estonia
GDP (million USD) (2023)	399,648.83	593,267.70	404,198.76	3,340,032.38	40,744.85
Demography					
Population size (2023)	34,308,530	10,536,630	5,946,950	68,350,000	1,366,190
Land area (sq km) (2021)	328,550.0	407,283.5	40,000	241,930.0	42,750
Population density (people per sq km of land area) (2021)	102	26	146	277	31
Healthcare system					
Coverage	Universal	Universal	Universal	Universal	Universal
Funding model	Public	Public	Public	Public	Public
Main source of funding	Tax	Tax	Tax	Tax	Insurance
Healthcare expenditure (% of GDP) (2022)	4.38 (2021)	10.67	9.5	11.34	6.94
Life expectancy at birth (2022)	76	83	81	82	78
Doctors per 10,000 population (2020)	22.3	43.1	44	30.4	34.8

Sweden

Sweden, which is one of the earliest countries in the world to have a national digitalisation agenda, began to develop parallel information systems for use by physicians and telemedicine applications in 1989 which subsequently in the 1990s, progressed into the creation of regional networks for sharing clinical information and developing e-prescription as well as home care systems. (87,89) The Patient Data Act that was enacted in 2008 allowed individuals to have direct access to their medical records online. (89) Despite having a healthcare system that is financed by public funds, Sweden's healthcare system is decentralised, thus allowing regional decisions. (89,90) In 2000, the "An Information Society for All" became the country's first national ICT policy with the objective to make Sweden the first country in the world to have an all-inclusive information society. (90,91)

In 2006, the government of Sweden published the National Strategy for eHealth which identified six action areas which focused on establishing better basic conditions for ICT in health and elderly care as well as to improve e-health solutions and adapt these to patient needs. (87,90) In 2016, the government then launched the Vision for eHealth 2025 which aims to make Sweden a world leader in e-health by 2025. (92)

Denmark

Denmark began to embark on e-health projects in the late 1980s with several projects aiming to interchange clinical data in electronic form. (87) MedCom, which was first introduced in 1994, was a non-profit cooperation between Danish authorities, organisations, and private firms linked to the Danish healthcare sector. (87,93,94) The government then launched the Danish Action Plan for EHR in 1996, followed by the National Strategy for IT in the Danish Hospital System 2000-2002 followed by the National IT Strategy for the Danish Health Care System 2003-2007. (93)

In 2003, "Sundhed.dk", a public health portal was established by the Danish Regions, Ministry of Health and Prevention, Local Government Denmark and the Association of Danish Pharmacies. It facilitates communication between healthcare practitioners and patients by allowing a single point of access to information. Individuals are able to view their medical records as well as manage their appointments with the general practitioner and renew their prescriptions. On the other hand, healthcare practitioners are also able to view the records of their own patients. (93,94) In 2004, the general practitioners in Denmark were mandated to use computers and EMR systems that are compliant with the standards set by MedCom for the purposes of managing patients' clinical notes, prescription lists, diagnostic images and laboratory test results as well as sending reminders to patients. (94)

Rather than focusing on operational goals, the National Strategy for Digitalisation of the Danish Healthcare Service 2008-2012 was aimed more on strategic goals with focus on consolidation of IT systems and facilitation of data sharing and exchange. (95) "Making eHealth Work - National Strategy for Digitalisation of the Danish

Healthcare Sector 2013-2017” was aimed to accelerate digitalisation, utilising digital tools as a more cost-effective health solution. (95,96) The most recent policy, the “A Coherent and Trustworthy Health Network for All - Digital Health Strategy 2018–2022” has a dual focus that is to prioritise the individuals’ healthcare needs and to improve the work burden for the healthcare staff. (95,97)

The United Kingdom

The United Kingdom’s healthcare system, upon which the Malaysian healthcare system was modelled after, had its first national health information technology strategy published in 1992 called “Getting Better with Information”. The objective was to provide a patient-centred approach by using information technology to support care and communications through an integrated operational clinical system. (98) However, healthcare services have been devolved as powers were transferred to the Scottish parliament, Welsh Senedd and the Northern Ireland assembly respectively in 1999, thus causing the healthcare policies, to evolve differently from one another. (99)

“Information for Health” provided a health information corporate strategy proposal for NHS England for the 1998-2005 period, setting out plans for EHR, electronic prescribing and online information services for patients. (87,98,100) However, the National Health Service Reform, introduced in 2004, included a funding package, thus resulting in separate plans being developed for Scotland, Wales and Northern Ireland, based on their local needs. (100–103)

While there is no common or central policy that dictates the direction of each of the NHS digital health policies, there is a common theme to leverage on technology to enhance the delivery of healthcare services throughout the nations. This includes the aim to have comprehensive and integrated digital health records which will allow each individual to have a single health record as well as to increase the adoption of e-prescription and telemedicine services. (100–103)

Estonia

Estonia, which is widely known as a highly digitalised and innovative country, began their healthcare system reforms after regaining independence in 1991. The reform started with the establishment of a social health insurance model where funds were collected through a special tax specifically meant for healthcare services. The electronic data management was also launched in the 1990s and healthcare providers were required to submit billing data electronically to receive funding. (104)

Generally considered to be the first country in the world to have a nationwide implementation of EHR, the Estonian Electronic Health Record System which virtually registers all residents’ medical history from birth to death was launched in 2008. (105) In 2013, The Estonian Health Insurance Fund (EHIF) began to allow payments for e-consultations, in which the patients would not have to go to the specialist care provider

as the system allows the family doctors to consult with the specialists through the health information system. (88) In 2016, Estonia became the first country in the world to use blockchain technology on a national scale to secure the health records in the country. (106)

Implementation progress: a comparative discussion

The divergent paths of digital health implementation between Malaysia and the studied countries are evident in both policy execution and outcomes. Malaysia has embarked on the digital health agenda relatively early compared to global trends, with nationwide ICT policies being introduced in the 1990s, implementation of paperless hospitals by the end of 1990s, and early planning for integrated lifetime medical records in 1997. (67,68)

By 2008, Estonia had achieved nationwide EHR implementation, and Denmark had mandated EMR use for all general practitioners by 2004. Despite Malaysia initiating its digital health agenda in the 1990s, around the same time as these countries, the progress of Malaysia's digital health adoption remains limited. In 2019, only 24% of MoH hospitals (35 out of 145) equipped with a Hospital Information System (HIS) and 7% of health clinics (118 of 1,703) using a Clinical Information System (CIS). (107)

The implementation approaches of digital health initiatives appear to be linked to the structure of each country's healthcare system structure and governance. Denmark and Estonia demonstrate strong centralised implementation, with their governments providing clear vision and coordinated national policies. For example, Denmark's mandate for EMR adoption by general practitioners and Estonia's nationwide EHR implementation show the effectiveness of centralised direction. Sweden, despite having a decentralised healthcare delivery system, maintains strong central policy direction through national strategies like Vision for eHealth 2025. The United Kingdom presents a contrasting model where healthcare devolution to Scotland, Wales, and Northern Ireland has led to distinct regional digitalisation strategies, though sharing common objectives. It has been shown that being part of the government agenda plays a role in ensuring a successful implementation of the ICT projects but this is also dependent on the government's budget allocation and restrictions. (64,68,87)

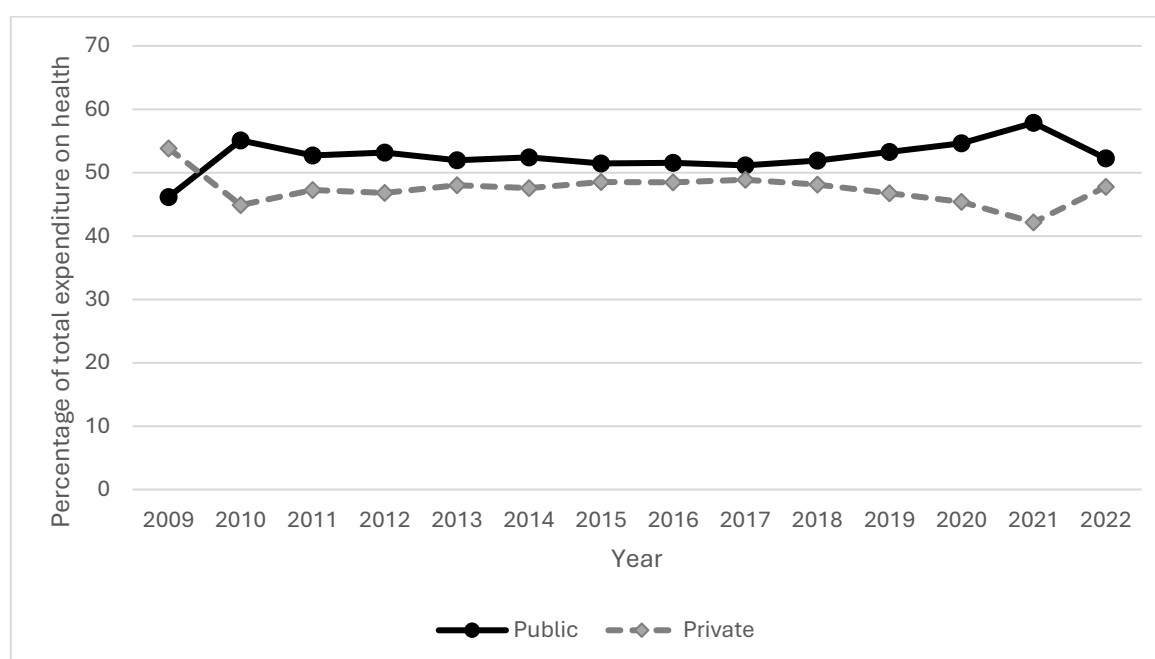
4.5 Sectoral divergence and innovation pathways

Malaysia's implementation journey is distinctly shaped by its dual public-private healthcare system. While the Ministry of Health provides policy direction, the implementation of digital health initiatives has progressed at different rates between the public and private sectors. The public sector's digitalisation efforts, constrained by government financial allocation, have shown slower progress. Conversely, the private sector, operating independently and driven by market forces, has demonstrated greater agility in adopting digital solutions.

Following the launch of the Privatisation Master Plan which included the healthcare sector in 1991, Malaysia began to attempt to shift the role of the Ministry of Health from a healthcare provider towards a role more focused on policy-making and regulatory matters. The privatisation policy led to a boom in the private healthcare industry with more people opting to pay for the services in the private healthcare sector, thus causing a shift in balance in the national expenditure in healthcare between the public and private sector. (108) The rapid growth of the private healthcare industry also saw the promotion of healthcare tourism as an important economic activity in the country. This led to the establishment of the Malaysia Healthcare Travel Council (MHTC) in 2009 which would take the leading role in facilitating further growth in health tourism activities in the country. (108,109)

Figure 2 highlights the shifting proportion of total health expenditure between the public and private sectors in Malaysia over the period 2009-2022.

Figure 2: Public and private healthcare expenditure, Malaysia (2009-2022)



Data source: Ministry of Health Malaysia's annual publication of "Health Facts" for years 2009 – 2022.

The divergent digitalisation trajectories between public and private healthcare sectors in Malaysia have created a striking contrast in technological adoption. While the Ministry of Health hospitals show limited digital implementation, private healthcare providers have embraced comprehensive digitalisation, extending beyond basic electronic medical records to encompass innovative smart hospital initiatives. This advanced digital adoption by private healthcare providers appears driven by the

competitive imperatives of international healthcare tourism and the need to maintain global service standards.

Private healthcare institutions' commitment to digital transformation is evidenced by their recognition in international healthcare excellence awards. For instance, at the Healthcare Asia Awards 2024, Sunway Home Healthcare, which is part of the private healthcare group Sunway Healthcare, received the Home-care Initiative of the Year award for their digitally enabled home-based medical services while ParkCity Medical Centre was acknowledged with the Smart Hospital Initiative of the Year award. (110,111) These accolades reflect not only technological advancement but also the private sector's strategic alignment of digital capabilities with service delivery excellence.

4.6 A growing presence of the digital health industry in the private healthcare sector in Malaysia

While traditional healthcare delivery models continue to evolve through government initiatives, Malaysia has witnessed the emergence of disruptive digital health innovations, primarily driven by private sector entrepreneurship. These innovations, operating parallel to established healthcare frameworks, are fundamentally reshaping service delivery patterns and patient engagement models.

The Malaysia Digital Economy Blueprint, which was launched under the Twelfth Malaysia Plan (2021-2025) had identified healthcare as one of the sectoral initiatives that would become a focus under the blueprint. While the blueprint itself does not outline any specific project that is related to the private healthcare industry, the coverage of the blueprint itself as a national document is very comprehensive. It covers all the aspects needed to set up a conducive ecosystem for the implementation of digital and communication technology, especially in terms of infrastructure development that would facilitate growth in any digitalisation agenda, regardless of sector. (112) The Malaysia National Artificial Intelligence Roadmap (2021-2025) also identified healthcare to be one of the priority areas with four projects, including a project on personalised healthcare, outlined under the sector. (113)

The healthcare technology startup ecosystem has emerged as a significant force in transforming traditional healthcare delivery models. These enterprises have identified and exploited gaps in conventional healthcare services, introducing novel solutions that challenge established practices. Digital wellness platforms and virtual healthcare services have gained particular traction, demonstrating the market's readiness for alternative healthcare delivery models. (62)

BookDoc exemplifies this disruptive transformation. Launched in 2015 as a digital platform connecting patients with healthcare professionals, it has evolved into a comprehensive health technology company operating across five countries. The platform's success in reimagining healthcare delivery through virtual services and

innovative public health interventions for lifestyle-related diseases has garnered international recognition, validating the viability of disruptive healthcare models. (114)

Similarly, DoctorOnCall has disrupted traditional healthcare delivery by creating an integrated digital ecosystem encompassing virtual consultations, e-prescriptions, and medication delivery. Its strategic alliance with the Malaysia Healthcare Travel Council (MHTC) represents a significant convergence of disruptive technology with established healthcare institutions, demonstrating how digital innovations can enhance and complement traditional healthcare services. (115)

These disruptive healthcare services are not merely digitising existing processes but are fundamentally reimagining healthcare delivery models. By leveraging technology to address accessibility, convenience, and efficiency challenges, these platforms are creating new value propositions in Malaysia's healthcare ecosystem, potentially bridging the service gaps between public and private healthcare sectors.

4.7 Regulatory gaps and governance challenges

Despite the dynamic growth of digital health services in Malaysia's private sector, regulatory uncertainty emerges as a significant barrier to innovation. The absence of clear regulatory frameworks has been consistently identified as a primary obstacle to technological advancement in healthcare, potentially constraining the sector's transformative potential. (61,116)

The Malaysian government has responded to these regulatory challenges through innovative regulatory mechanisms. The Ministry of Finance's launch of the National Regulatory Sandbox (NRS) in 2018 represented a significant step toward addressing regulatory uncertainties surrounding emerging technologies. (116) This was followed by the Ministry of Science, Technology and Innovation's (MOSTI) introduction of the National Technology and Innovation Sandbox (NTIS) in 2020. (116) While distinct in their focus, these regulatory sandboxes share a common objective: creating protected environments where innovations can be tested and refined. These initiatives facilitate collaboration between innovators, researchers, and entrepreneurs, enabling them to navigate technical, regulatory, and financial challenges while accelerating the commercialisation of their solutions. (116–118)

The evolution of Malaysia's sandbox ecosystem demonstrates increasing sophistication in regulatory innovation. The recent announcement of a strategic collaboration between the Malaysian Research Accelerator for Technology and Innovation (MRANTI) and NVIDIA to establish an AI Sandbox Pilot Programme under NTIS in April 2024 exemplifies this progression. (119) However, despite these positive developments, significant gaps remain, particularly in securing active participation from regulatory bodies and agencies. (118) This limited engagement from regulatory stakeholders potentially hampers the effectiveness of these sandbox initiatives in facilitating meaningful regulatory reform.

The contrast between rapid technological innovation and evolving regulatory frameworks highlights a critical challenge in Malaysia's digital health transformation journey. While regulatory sandboxes provide temporary solutions, the development of comprehensive, permanent regulatory frameworks remains essential for sustainable growth in digital health services.

4.8 Policy and practice implications

The evolution of Malaysia's digital health policies underscores the necessity for a more cohesive and future-proof governance framework. The digitalisation gap between the public and private sectors, if left unaddressed, may lead to a fragmented and inequitable healthcare landscape. Lessons from Denmark and Estonia highlight the value of centralised strategic leadership in driving successful digital health transformation. Future policymaking should prioritise building a sustainable, adaptive regulatory ecosystem that anticipates emerging technologies rather than retroactively responding to them. These insights are relevant not only for Malaysia, but also for other countries grappling with mixed healthcare systems and digitalisation challenges.

These implications underscore the importance of not only supportive policies, but also coherent governance structures that can translate strategic intent into practical, secure, and inclusive digital health solutions.

4.9 Conclusion

This comparative analysis highlights the complex dynamics shaping the implementation of healthcare digitalisation policies, influenced by governance structures, regulatory frameworks, and mechanisms of execution. While countries such as Estonia and Denmark have made significant progress through centralised digital health strategies, Malaysia's trajectory reflects a unique dual-track public-private system.

Malaysia's experience illustrates both the challenges and opportunities inherent in a mixed healthcare model. Public sector digitalisation has progressed at a slower pace, constrained by financial and institutional limitations. In contrast, the private sector has emerged as a key driver of advanced digital health innovation, propelled by market forces and industrial competitiveness. Concurrently, health technology startups have introduced disruptive service models, transforming conventional healthcare service delivery into increasingly virtual and platform-based environments.

This evolution suggests that the government's role in digital transformation must extend beyond direct implementation. It also entails cultivating an enabling infrastructure that fosters innovation across the healthcare ecosystem. However, regulatory uncertainty remains a significant obstacle for emerging technologies that challenge traditional models of care. Regulatory sandboxes may offer a promising

interim solution, but a comprehensive, long-term framework that can support innovation while safeguarding the public interest is still required.

The rise of disruptive healthcare services underscores the urgency of developing an adaptive, responsive regulatory environment that encourages innovation without compromising quality, safety, or equity. Malaysia's future success in digital health will hinge not only on its ability to bridge the digital divide between public and private sectors, but also on its capacity to embed governance structures that align innovation with accountability. A meaningful nationwide transformation will depend on coordinated legal, institutional, and technical alignment.

The evolution of Malaysia's digital health policy reveals a progressively enabling environment for innovation. However, the translation of policy ambition into secure and accountable health data practices requires a deeper examination of governance structures such as legal, institutional, and technical, which are addressed in the following chapter.

Chapter 5

Governance Foundations: Legal, institutional, and policy context for wearable health data

5.1 Introduction

As wearable technologies become more integrated into personal health routines and clinical decision-making, the governance of PGHD has emerged as a critical concern. Effective governance frameworks must strike a balance between the need for innovation and interoperability with legal mandates for privacy, security, and accountability.

This chapter examines the governance landscape surrounding PGHD, focusing on four interrelated dimensions:

- The legal and regulatory foundations that shape healthcare service delivery and data protection in Malaysia.
- The frameworks governing data use and sharing in the Malaysian context.
- The institutional arrangements and stakeholder roles across public agencies, technology companies and digital health innovators.
- Selected international frameworks that offer comparative insights and instructive approaches to PGHD governance.

The analysis is grounded in a triangulation of legal texts, policy documents, institutional guidelines, and interpretive insights derived from the author's professional familiarity with Malaysia's public health governance ecosystem. Where appropriate, the chapter highlights key challenges, coordination gaps, and normative tensions between public interest, individual autonomy, and corporate control.

The following sections examine how Malaysia's legal, institutional, and policy structures interact with the realities of wearable health technologies. These

foundations provide the governance context upon which technical implementation mechanisms (discussed in Chapter 6) should be built.

5.2 Legal and regulatory landscape in Malaysia

5.2.1 Healthcare service regulations: Practitioners, facilities, pharmaceuticals and devices

Malaysia's healthcare regulatory landscape is governed by a series of sector-specific laws developed to oversee clinical practice, healthcare facilities, medical devices, and pharmaceuticals. These include the Medical Act 1971 for doctors, the Nurses Act 1950 for nursing professionals and the Private Healthcare Facilities and Services Act 1998 for institutional licensing, among others. Table 4 summarises the key legal instruments that are relevant to healthcare service regulation in Malaysia. (120–128)

Table 4: Key Malaysian legal instruments relevant to healthcare service regulation

Domain	Law / Regulation	Scope / Focus
Medical practitioners	Medical Act 1971 [Act 50]	Governs the registration and practice of medical doctors through the Malaysia Medical Council.
	Nurses Act 1950 [Act 14]	Governs the registration and practice of nurses and midwives through the Nursing Board.
	Medical Assistants (Registration) Act 1977 [Act 180]	Governs the registration and practice of assistant medical officers through the Medical Assistants Board.
	Allied Health Professions Act 2016 [Act 774]	Governs the registration and practice of allied health professionals through the Malaysian Allied Health Professions Council.
Healthcare facilities	Private Healthcare Facilities and Services Act 1998 [Act 586]	Regulates the licensing and operations of private hospitals, clinics and other medical institutions.

Domain	Law / Regulation	Scope / Focus
Pharmaceutical	Poisons Act 1952 [Act 366]	Regulates the classification, possession, prescription, sale, and supply of scheduled poisons and medicinal substances by authorised professionals.
	Sale of Drugs Act 1952 [Act 368]	Provides the legal framework for the registration, importation, manufacture, and licensing of pharmaceutical products, administered through the Drug Control Authority.
	Medicines (Advertisement and Sale) Act 1956 [Act 290]	Prohibits misleading advertisements and promotional activities related to medicines and health treatments and governs marketing claims directed at the public.
Medical devices	Medical Device Act 2012 [Act 737]	Regulates the classification, registration, importation, and post-market control of medical devices through the Medical Device Authority.

While these frameworks are robust in safeguarding professional standards and patient safety, they are primarily focused on care delivered within formal institutions. None of the instruments engage directly with data governance issues, such as the collection, transmission, processing, or reuse of PGHD, nor do they account for the evolving role of consumers as data generators and active participants in health monitoring.

Therefore, as digital technologies increasingly blur the lines between clinical care and consumer health, there is a growing reliance on cross-sectoral data governance frameworks to safeguard personal health information. The following section explores these horizontal legal instruments, including the Personal Data Protection Act, the National Archives Act, and the Communications and Multimedia Act, which collectively form the foundation of Malaysia's legal approach to digital health data.

5.2.2 Regulatory framework for personal data and digital health information

Malaysia lacks a dedicated health data statute. Instead, regulatory responsibilities are fragmented across several legal frameworks that apply to medical records, digital infrastructure, and personal data more broadly. This fragmentation creates specific governance challenges for PGHD, which operates across traditional regulatory boundaries.

Medical records in public and private healthcare

For private healthcare providers, medical record-keeping is governed by the *Private Healthcare Facilities and Services Regulations 2006*, issued under the Private Healthcare Facilities and Services Act 1998 [Act 586]. (129) However, these requirements apply only to licensed healthcare facilities and do not extend to standalone mobile applications or consumer wearables used outside clinical settings.

In the public sector, record-keeping is governed by the *Garis Panduan Pengendalian dan Pengurusan Rekod Perubatan Pesakit di Fasilitas KKM* (Guidelines for the Handling and Management of Patient Medical Records at MoH Facilities). (130) These guidelines, issued by the Ministry of Health, detail procedures for documentation, classification, storage, access, and disposal of patient records. Their legal authority is derived from the *National Archives Act 2003* [Act 629], which governs public sector record management. These guidelines govern institutional records but do not address data generated by consumer devices.

This regulatory structure creates a governance gap where consumer-generated health data operates outside existing medical record frameworks, requiring reliance on general data protection laws examined below.

Personal Data Protection Act 2010 and 2024 Amendments

The *Personal Data Protection Act 2010* [Act 709] is the principal legislation governing personal data processing in the private sector. (131) Enacted in response to Malaysia's growing digital economy and rising concerns over credit card fraud, identity theft, and unauthorised selling of personal data without user consent, the PDPA was designed to strengthen consumer confidence in business transactions and e-commerce. (132) It establishes core data protection principles such as consent, notice, purpose limitation, access, correction, and security, which apply to any private entity engaged in commercial transactions involving personal data. However, the PDPA explicitly excludes public agencies from its scope, creating a bifurcated legal environment in which health data managed by the MoH is not subject to the same protections as that held by private platforms. (132)

In 2024, the PDPA was amended via Act A1727, introducing several structural reforms intended to align Malaysia's framework more closely with global standards such as the European Union's General Data Protection Regulation (EU GDPR). (133,134) These amendments introduced clearer role definitions and responsibilities, modest expansions of data subject rights, as well as enhanced organisational accountability mechanisms. (134)

Key changes include:

- Terminology alignment: All references to “*data user*” were replaced with “data controller” and the term “data processor” was formally defined, in line with international norms. This change clarifies the distinct roles in the data processing chain, a necessary step toward improving access governance.
- New obligations for “*data processors*”: Prior to the 2024 amendment, the responsibilities of data processors were not clearly defined. Under the new amendment, Section 5 of Act A1727 introduced a new obligation under the Security Principle (defined under Section 9 of Act 709), stating:

“A data processor shall, when processing personal data on behalf of a data controller, comply with the security principle as if it were a data controller.”

(Act A1727, s.5)

This marks a structural shift in accountability, extending legal responsibility beyond controllers to third-party service providers which is a significant move for PGHD ecosystems that rely heavily on outsourced platforms and cloud services.

- Right to data portability: A new section 43A which was added in the 2024 amendments, introduces a form of data portability:

“A data subject may request the data controller to transmit his personal data to another data controller of his choice [...] by way of electronic means, subject to technical feasibility.”

(Act A1727, s.43A)

This provision reflects similar rights under the GDPR but it is framed as a request-based mechanism, rather than a direct entitlement, and its enforceability remains uncertain, particularly when dealing with PGHD held by foreign platforms.

- Mandatory appointment of Data Protection Officers (DPOs): The amendment also introduced Section 12A, requiring organisations to formalise internal accountability mechanisms:

“A data controller shall appoint one or more data protection officers to ensure compliance with the provisions of this Act.”

(Act A1727, s.12A)

While this may improve internal compliance structures, it does not necessarily translate to greater transparency or meaningful access for individuals.

Despite these reforms, the amended PDPA still lacks sector-specific provisions for health data, offering no tailored guidance on data collected through wearable technologies or digital health platforms. Moreover, as the Act does not apply to public sector bodies, there remains no overarching framework to ensure consistent protection or access control across Malaysia's fragmented digital health ecosystem. Crucially, the PDPA also lacks extraterritorial enforcement power, raising questions about its applicability to foreign technology vendors who collect and process PGHD generated by Malaysian residents.

The 2024 amendments have modernised Malaysia's data governance framework but its contribution towards the establishment of PGHD governance remains limited. The emphasis on request-based rights, combined with jurisdictional gaps and institutional exclusions, reinforces a controller-centric model in which individuals remain dependent on third parties to exercise limited forms of data access and portability.

Communications and Multimedia Act 1998

The Communications and Multimedia Act 1998 provides the foundational legal framework for regulating Malaysia's converging communications and multimedia industries. It covers network facilities, network services, applications services, and content applications services, establishing comprehensive governance over digital infrastructure. The Act establishes the regulatory framework for the Malaysian Communications and Multimedia Commission (MCMC) as the primary regulatory body, empowered to oversee licensing, industry standards, and compliance enforcement. It sets out principles for market conduct, consumer protection, fair competition, and includes provisions for content regulation and cybersecurity. (135)

Although the Communications and Multimedia Act 1998 does not regulate health data directly, it establishes foundational governance over the digital infrastructure and services through which PGHD may be transmitted or processed. As such, it forms part of the broader regulatory ecosystem that indirectly shapes technical trust, security, and interoperability for digital health applications.

Data Sharing Act 2015

The Data Sharing Act 2025, which was enacted in 2025, represents a key step forward in Malaysia's data governance framework. Its primary objective is to facilitate secure and accountable data exchange between public sector agencies, enhancing inter-agency coordination for data-driven governance. While the Act introduces mechanisms for secure data transfer, accountability, and shared infrastructure, its scope is primarily focused on government entities and public-sector applications, though it does allow for private sector participation through certified Data Sharing Entities. (136)

As such, the Act's coverage of PGHD or private sector health platforms remains limited. Without comprehensive provisions for individual consent, third-party data analytics, or interoperability requirements specific to health data, the Act's direct relevance to PGHD governance remains minimal, though it may provide a framework for future integration with private-sector digital health services.

This fragmented regulatory landscape, where PGHD falls between healthcare, telecommunications, and data protection frameworks, creates the governance gaps that the following section examines through institutional analysis.

5.3 Digital health governance in Malaysia: Synthesis of institutional roles

This section examines the institutional arrangements that operationalise Malaysia's digital health governance frameworks. Understanding which entities are involved and how they coordinate, or conflict is essential for identifying gaps in accountability, enforcement, and policy coherence.

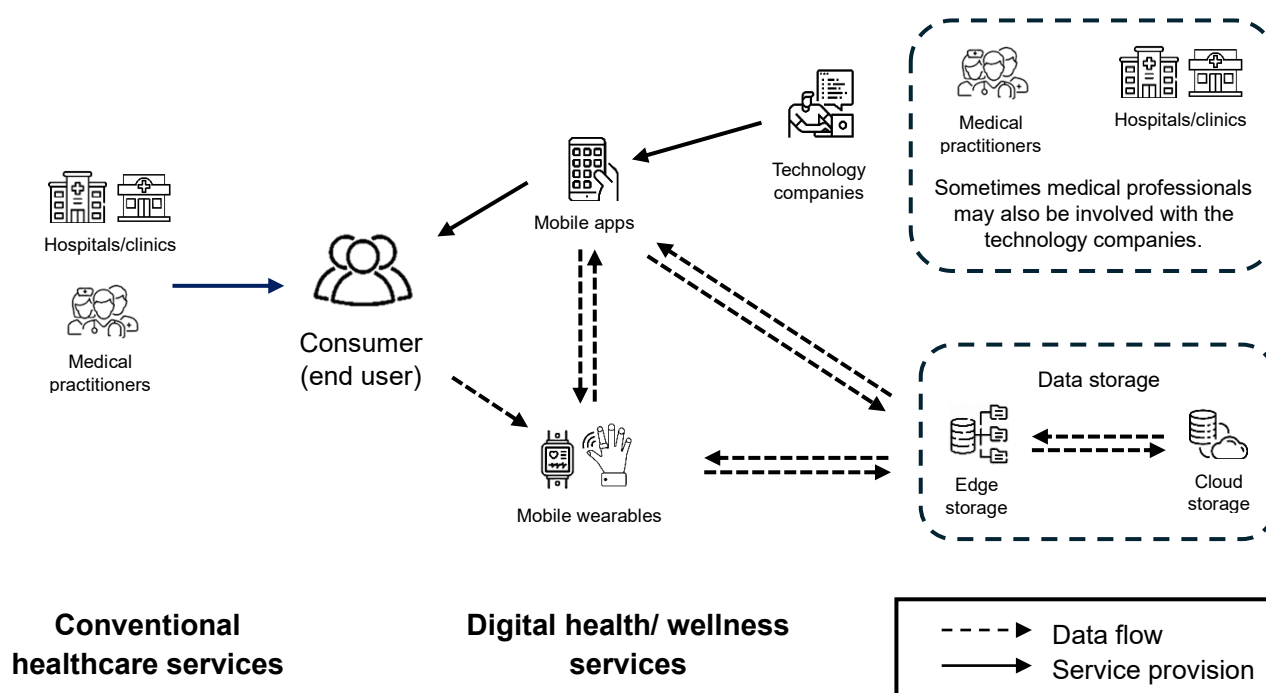
5.3.1 Overview of Malaysia's digital health ecosystem

Malaysia's digital health ecosystem involves multiple stakeholders with overlapping jurisdictions, diverse business models, and varying degrees of regulatory oversight. Unlike traditional healthcare systems with clear hierarchical structures, this ecosystem spans both conventional healthcare delivery and emerging digital health services.

Figure 3 illustrates this ecosystem structure, highlighting the disconnect between conventional healthcare services and digital health platforms. Traditional healthcare institutions operate within established regulatory frameworks, while digital health platforms, wearable device manufacturers, and cloud storage providers function largely outside these governance structures.

This creates significant governance challenges for PGHD, which crosses multiple organisational boundaries and regulatory frameworks. The following sections examine the key institutional actors such as public agencies, private sector stakeholders, and their coordination challenges that shape PGHD governance in Malaysia.

Figure 3: Institutional and technological actors in Malaysia's healthcare ecosystem



5.3.2 Key public institutions related to digital health governance ecosystem in Malaysia

Malaysia's digital health governance ecosystem is evolving in tandem with broader institutional reforms in national digital governance. In 2023, the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) was officially restructured as Jabatan Digital Negara (National Digital Department) (JDN) and placed under the newly established Ministry of Digital. This transition reflects the government's ambition to centralise and strengthen oversight of digital transformation initiatives across all sectors, including healthcare. (137)

As the national lead agency for public sector digitalisation, JDN retains MAMPU's original mandate, with a primary focus on infrastructure, administrative efficiency, and cross-government ICT coordination, including e-government, cloud adoption, ICT standardisation, and inter-agency data interoperability. While its scope spans multiple sectors, its priorities remain largely administrative, and it does not currently address health-sector-specific data standards, PGHD, or the integration of consumer wearables into national health systems.

The Ministry of Health Malaysia (MoH) operates within this evolving digital governance landscape as the primary steward of the national healthcare system and plays a central role in the governance of institutional medical records and public health data infrastructure. Through its administrative and clinical divisions, the MoH oversees public healthcare delivery, regulates healthcare facilities and professional practice, and maintains data systems such as the Malaysian Health Data Warehouse

(MyHDW). It also issues operational guidance, including the *Garis Panduan Pengendalian dan Pengurusan Rekod Perubatan Pesakit di Fasilitas KKM* (Guidelines for the Handling and Management of Patient Medical Records at MoH Facilities), which governs the documentation, storage, and retention of patient records in public health facilities.

Two specialised regulatory bodies under the MoH also play important roles in digital health governance, namely the Medical Device Authority (MDA) and the National Pharmaceutical Regulatory Agency (NPRA).

The MDA regulates medical devices under the Medical Device Act 2012, including certain digital health products such as diagnostic wearables and remote monitoring tools classified as medical devices. However, consumer-grade wearables used for general wellness or fitness tracking fall outside MDA's scope, creating a regulatory gap where devices generating health-related data operate without medical device oversight.

Meanwhile, the NPRA oversees pharmaceuticals and product advertisements under the Medicines (Advertisement and Sale) Act 1956. While its primary focus is medicinal products, it has indirect oversight of health claims made by digital applications and wearables. Like MDA, its mandate does not explicitly cover PGHD, nor does it address post-market surveillance of data integrity or privacy standards in health software systems.

This institutional landscape reveals significant coordination challenges. While JDN focuses on digital infrastructure and the MoH manages healthcare data systems, no single agency has comprehensive oversight of PGHD flowing between consumer devices and health systems. Consumer wearables generating health data operate in a regulatory space between medical device oversight and general data protection, with unclear accountability for data quality, user privacy, or system interoperability.

5.3.3 Cross-sectoral and industry stakeholders

In addition to public institutions, Malaysia's digital health landscape involves a wide range of private-sector and cross-sectoral stakeholders. These actors often operate outside traditional healthcare regulatory structures yet play a central role in shaping how PGHD is collected, processed, and applied. Unlike institutional health data, PGHD typically originates in consumer-facing platforms and devices, creating regulatory and accountability gaps in data protection, interoperability, and consent governance that existing institutional frameworks cannot adequately address.

Wearable Device Vendors

The Malaysian wearable health device ecosystem is largely shaped by global companies such as Fitbit, Apple, Garmin, Huawei, and Samsung, whose products are

widely used by consumers worldwide. These vendors collect high volumes of health-related data through smartwatches, fitness trackers, and health-focused apps, typically without direct integration into formal healthcare systems.

While these companies typically operate under consumer protection and privacy laws in their respective jurisdictions, their operations in Malaysia are generally subject to the broad provisions of the Personal Data Protection Act (PDPA). As discussed in Section 5.2.2, the PDPA's lack of sector-specific provisions for health data and unclear extraterritorial enforcement create significant regulatory gaps. Most wearable platforms manage health data through proprietary user agreements and operate independently from Malaysia's healthcare governance mechanisms, with no obligation for clinical validation, national interoperability, or integration with existing healthcare institutions. This creates a parallel health data ecosystem that functions outside established governance structures.

For example, while a patient's blood pressure readings taken in a clinic are subject to MoH record-keeping guidelines and PDPA exemptions for public agencies, the same patient's continuous blood pressure monitoring via a smartwatch operates under different, or potentially no governance frameworks.

Digital Health Startups and App Developers

Malaysia is seeing the emergence of digital health startups offering remote monitoring, teleconsultation, personal health tracking, and AI-driven diagnostics. These platforms increasingly rely on PGHD to personalise services or offer predictive analytics. However, there are few sector-specific standards or regulatory frameworks guiding how these companies manage data quality, user consent, or integration with national health records. Most operate under the general obligations of the PDPA and may fall into regulatory grey areas if their applications straddle the line between lifestyle use and clinical functionality.

Cloud Providers and Digital Infrastructure Companies

Major technology firms such as Amazon Web Services (AWS), Google Cloud, and Microsoft Azure provide backend infrastructure for health platforms, serving both consumer-facing applications and enterprise health systems. Acting as data processors for PGHD stored or analysed through cloud-hosted applications, these entities straddle both consumer and institutional sides of the health data ecosystem. They enable scalable and real-time data operations but are often governed only through contractual agreements between the cloud service and the health data controller. There is no public registry, certification, or formal oversight body in Malaysia to ensure that cloud-hosted PGHD complies with security, localisation, or sector-

specific governance requirements. This creates a governance gap where critical health data infrastructure operates with minimal regulatory oversight.

These diverse private sector actors (device vendors, platform developers, and infrastructure providers) operate largely independently from both each other and Malaysia's public health institutions, creating a fragmented ecosystem where coordination and accountability remain limited.

5.3.4 Coordination challenges and fragmentation

Despite the growing number of stakeholders involved in digital health governance in Malaysia, institutional coordination remains limited. The governance of PGHD falls between multiple regulatory silos. Public institutions such as the Ministry of Health, the Medical Device Authority, and the National Pharmaceutical Regulatory Agency primarily focus on clinical care and regulated medical products, while agencies like JDN and the Ministry of Digital oversee broader infrastructure and digital transformation. These bodies operate with distinct mandates, limited interoperability, and no central authority responsible for the oversight of PGHD.

This fragmentation extends to the private sector, where platform developers, wearable vendors, and cloud service providers manage large volumes of PGHD with minimal coordination between themselves or alignment with national healthcare systems. Startups and digital health platforms often operate without formal pathways for data integration into public records or clinical workflows, while cloud infrastructure decisions such as server location or security standards are governed through private contractual terms rather than enforceable health-sector policies.

The result is a governance landscape where accountability is diffused, responsibilities are unclear, and critical decisions about health data collection, storage, access, and use are made outside formal public oversight mechanisms. Efforts to promote digitalisation, such as regulatory sandboxes and national blueprints, have facilitated innovation but have not addressed the structural gaps in data governance or the fragmentation between agencies. This limits Malaysia's ability to ensure data interoperability, user protection, and strategic alignment across public health, technology, and economic development goals.

5.4 Global approaches to digital health data governance

As Malaysia navigates the complexities of digital health transformation, it is instructive to examine how other jurisdictions have approached the governance of PGHD and wearable technologies.

This comparative analysis focuses on governance models and regulatory paradigms, examining how different jurisdictions approach the balance between individual rights, institutional responsibilities, and innovation incentives in digital health data

governance. The analysis prioritises understanding implementation mechanisms and their implications for technical architecture design.

Comparative insights offer valuable lessons on institutional design, legal safeguards, and technical mechanisms that can inform domestic reforms. While local contexts differ, international models highlight key principles that directly address the governance fragmentation identified in Malaysia: data portability, user agency, interoperability, and institutional coherence.

5.4.1 European Union: Rights-driven, interoperable frameworks

The European Union offers one of the most comprehensive and rights-driven models for personal data governance, with important implications for PGHD. The EU's rights-based approach prioritises individual data protection as a fundamental right under Article 8 of the Charter, implemented through comprehensive regulatory frameworks with significant enforcement penalties. (138) The General Data Protection Regulation (GDPR) serves as the legal backbone of the EU's digital health governance framework, establishing enforceable principles around data minimisation, purpose limitation, and accountability.

The GDPR creates a presumption against health data processing that differs fundamentally from sectoral approaches where protection depends on institutional context rather than data sensitivity. Article 9 establishes a general prohibition on processing health data by designating it as a "special category of personal data," with specific exceptions that must be satisfied:

“Processing of [...] data concerning health [...] shall be prohibited.”

(General Data Protection Regulation, Regulation (EU) 2016/679, Art. 9)

This prohibition can be lifted under Article 9(2)(a) if explicit consent is provided for specified purposes.

“The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.”

(General Data Protection Regulation, Regulation (EU) 2016/679, Art. 9(2)(a))

In addition, Article 20 of the GDPR introduces a legally binding right to data portability, stating:

“The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have

the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided [...]"

(General Data Protection Regulation, Regulation (EU) 2016/679, Art. 20)

While this appears to enable user control, its limitation to data "provided by" the data subject creates interpretive challenges for PGHD where platforms generate derivative insights through algorithmic processing. (139)

The GDPR's horizontal protections are further expanded by the European Health Data Space (EHDS), formally adopted in 2025. The EHDS demonstrates how European law adapts general privacy principles to domain-specific requirements while maintaining rights-based foundations. The regulation enables individuals to insert their data into electronic health records under strict consent controls (Article 5), and explicitly addresses wellness applications in Article 48(2), requiring that interoperability with EHR systems operate only through informed consent and explicit user selection.

"Natural persons [...] shall have the right to insert information in the EHR [...] through electronic health data access services or applications linked to those services. That information shall be clearly distinguishable as having been inserted by the natural person or by his or her representative."

(Regulation (EU) 2025/327, Art. 5)

"The interoperability of wellness applications with EHR systems shall not entail the automatic sharing of all or part of the health data from the wellness application with, or automatic transmission of all or part of such data to, the EHR system. The sharing or transmission of such data shall only be possible if it is in accordance with Article 5 and after consent is given by the natural person concerned and interoperability shall be limited exclusively to those purposes. The manufacturers of wellness applications claiming interoperability with an EHR system shall ensure that the natural person concerned is able to choose which categories of health data from the wellness application are to be inserted in the EHR system and the circumstances for the sharing or transmission of those categories of data."

(Regulation (EU) 2025/327, Art. 48(2))

This reveals the EU's governance philosophy: technical interoperability must be subordinated to user control mechanisms, creating a presumption that data integration requires active user direction rather than default sharing. Taken together, the GDPR and EHDS offer a cohesive model in which individual rights, data sensitivity, and

interoperable infrastructure are embedded into the legal architecture for digital health. Their combined provisions illustrate how PGHD can be legally recognised, protected, and conditionally integrated into formal health systems within a rights-preserving framework.

Complementing the GDPR and EHDS, the Artificial Intelligence Act (AI Act), adopted in 2024, introduces a risk-based regulatory framework for AI systems across the EU. The regulation classifies AI systems used in health and essential public services as high-risk due to their potential impact on individual rights and wellbeing, imposing stringent requirements including obligations for data quality, risk management, human oversight, and post-market monitoring. (140)

While the regulation does not specifically reference wearable devices or PGHD, its provisions apply to AI systems that are formally certified as medical devices under existing EU medical device regulations. However, most consumer-grade wearables and wellness applications fall outside this classification and thus remain largely unregulated under the AI Act. This gap mirrors challenges Malaysia faces with consumer wearables, though the EU's risk-based approach offers lessons for managing PGHD systems incorporating algorithmic decision-making.

The EU model demonstrates how comprehensive rights-based frameworks can address PGHD governance through three key mechanisms: special category protection for health data, mandatory user consent with granular control, and sector-specific frameworks that bridge general privacy law with health-specific requirements. However, this approach also reveals tensions between comprehensive protection and innovation flexibility that other jurisdictions have addressed differently.

This rights-driven approach provides strong individual protections and clear regulatory frameworks, but its complexity and compliance requirements may constrain rapid innovation. Understanding this trade-off becomes essential when examining how other jurisdictions have prioritised innovation over comprehensive protection.

5.4.2 United States: Innovation-led federated regulation

From a comparative governance perspective, the United States adopts a markedly different approach to digital health regulation compared to the European Union. Rather than the EU's unified, rights-based regulatory framework, the U.S. relies on a patchwork of sector-specific statutes, agency-level rules, and state-driven initiatives that collectively shape the legal treatment of PGHD. This federated and decentralised structure reflects the country's emphasis on innovation and market-driven development but results in uneven protections and limited coordination across the digital health ecosystem.

The primary federal regulation governing health data is the Health Insurance Portability and Accountability Act (HIPAA) of 1996. It was originally enacted to support insurance portability and facilitate administrative efficiency in healthcare billing and

reimbursement. As a result, HIPAA's Privacy and Security Rules focus predominantly on safeguarding health information within the context of clinical care and reimbursement. Its scope is limited to covered entities, including healthcare providers, along with their business associates. Its protections are tied to regulated health services and payment structures and therefore it permits data sharing for purposes such as treatment, payment, and healthcare operations. (141)

The U.S. Department of Health and Human Services (HHS) explicitly clarifies that these protections do not extend to health information managed outside this institutional framework. As stated in HHS guidance:

“The HIPAA Rules generally do not protect the privacy or security of your health information when it is accessed through or stored on your personal cell phones or tablets. The HIPAA Rules apply only when PHI is created, received, maintained, or transmitted by covered entities and business associates.” (142)

As a result, PGHD collected via consumer-facing wearables or mobile health applications typically falls outside HIPAA's jurisdiction unless the device is used within a clinical workflow or shares data with a covered entity. For example, health data generated by Apple Health or Fitbit users remains largely unregulated under HIPAA when used outside institutional care and confined to consumer-facing platforms. This institutional focus left significant gaps in consumer health technology governance, which subsequent legislation attempted to address through market-driven solutions.

The 21st Century Cures Act (2016) reflects a significant policy shift in the United States toward improving patient access to electronic health information (EHI) and facilitating data interoperability. From an implementation perspective, the Act's architects recognised that existing health information systems typically restricted patient access in ways that tied individuals to their current providers and insurance plans, necessitating regulatory intervention to enable true patient control over their data. (143) Section 4006 of the Act specifically addresses the role of health information exchanges (HIEs) in supporting patient access. Subsection 4006(c) directs:

“The Secretary shall use existing authorities to encourage partnerships between health information exchange organisations and networks and health care providers, health plans, and other appropriate entities with the goal of offering patients access to their electronic health information in a single, longitudinal format that is easy to understand, secure, and may be updated automatically.”

(21st Century Cures Act §4006(c), Public Law 114–255)

This statutory language underscores the government's commitment to enabling patient-directed data sharing across organisational boundaries, with an emphasis on usability, continuity, and security. Policymakers designed the Act to shift control of health information to patients themselves, recognising that healthcare data becomes significantly more useful when individuals can access and utilise it independently rather than through provider-controlled channels. (143)

Building on this mandate, the ONC (Office of the National Coordinator for Health Information Technology) Cures Act Final Rule which was published in 2020 to implement the interoperability provisions of the Act, interprets these obligations as extending beyond direct access to include data sharing with third-party applications or individuals. In explaining the rationale for new certification criteria, the Office of the National Coordinator stated:

“This final certification criterion is designed to align with section 4006(a) of the Cures Act, which requires the Secretary, in consultation with the National Coordinator, to promote policies that ensure that a patient's EHI is accessible to that patient and the patient's designees, in a manner that facilitates communication with the patient's health care providers and other individuals.”

(85 Fed. Reg. 25691)

This regulatory interpretation reinforces the Act's broader vision of consumer-directed data portability, allowing individuals not only to access their health data but also to transmit it to digital health services, personal health applications, or caregivers of their choice, through Application Programming Interface (API) as mentioned:

“As a Condition of Certification requirement in section 4002 of the Cures Act requires health IT developers to publish APIs that allow “health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law.” The Cures Act's API Condition of Certification requirement also states that a developer must, through an API, “provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.””

(85 Fed. Reg. 25647)

To ensure these patient access rights are meaningful in practice, the Act establishes strong prohibitions against information blocking. Section 4004 of the Cures Act added section 3022 to the Public Health Service Act, which the ONC Final Rule operationalised through 45 CFR 171.103, defining information blocking as:

"a practice that except as required by law or covered by an exception set forth in subparts B, C, or D of this part, is likely to interfere with access, exchange, or use of electronic health information."

(45 C.F.R. § 171.103)

This comprehensive framework, combining mandatory access rights, API requirements, and strong anti-blocking provisions, establishes a clear policy preference for consumer-directed data sharing over paternalistic restrictions imposed in the name of privacy protection.

However, while federal initiatives prioritised data access and interoperability, state-level regulations emerged to address the privacy protection gaps this approach created. The California Consumer Privacy Act (CCPA), which came into effect in 2020, represents the most comprehensive state-level privacy legislation in the United States. The CCPA grants California residents specific rights over their personal information, including health data collected by businesses that meet certain revenue or data volume thresholds. (144) The California Privacy Rights Act (CPRA), which was implemented in 2023, significantly expands the CCPA's provisions by introducing the concept of "sensitive personal information," which includes health data, biometric information, and information concerning health diagnosis, condition, or treatment. (145)

Under the CCPA, as amended by CPRA, consumers have enforceable rights to access, delete, opt out of the sale of their personal information, with CPRA adding rights to correct and limit the use of their personal information. These rights apply to consumer-grade wearables and health applications operated by businesses meeting the statutory thresholds, creating a regulatory framework that extends beyond HIPAA's institutional focus. (144,145)

The CPRA amended, rather than replaced the CCPA, so both sets of provisions now operate together under the California Privacy Protection Agency (CPPA), established by the CPRA to enforce compliance through administrative fines and consumer complaints. However, it lacks the clinical expertise or sectoral focus of health data authorities. This creates a governance model where health data protection depends on general privacy enforcement rather than specialised oversight attuned to the unique risks and opportunities in digital health.

This horizontal privacy approach contrasts sharply with the EU's health-specific protections, demonstrating how different jurisdictions balance innovation incentives with consumer protection through distinct institutional mechanisms.

Despite these limitations, the CCPA/CPRA model demonstrates how comprehensive state-level privacy legislation can address regulatory gaps left by federal sectoral laws like HIPAA. For jurisdictions like Malaysia, where PGHD falls outside existing health data governance frameworks, California's approach demonstrates the potential of

horizontal privacy legislation to provide baseline protections while more targeted, sector-specific regulations evolve.

Overall, the U.S. regulatory environment supports rapid innovation in digital health, particularly through API-based data exchange and market incentives for remote monitoring and analytics services. While it lacks a unified legal framework for PGHD, recent developments emphasise patient access, data portability, and autonomy in managing personal health information. In contrast, the European Union's rights-based framework prioritises data protection through comprehensive privacy safeguards and strong institutional oversight. Rather than viewing these approaches as oppositional, they can be seen as emphasising different dimensions of data rights: the EU model foregrounds the right to protection, while the U.S. increasingly promotes the right to access and autonomy. Both perspectives are critical to effective governance of PGHD, particularly as individuals become active participants in managing and sharing their own health data across diverse platforms and services.

5.5 Thematic insights and applicability to Malaysia

The thematic analysis of EU and US approaches reveals fundamentally different philosophical orientations toward data protection, innovation, and individual agency, yet these differences represent complementary rather than contradictory dimensions of data governance. These contrasting models offer valuable insights for Malaysia as it seeks to develop a coherent framework for PGHD governance that aligns with its unique healthcare system structure and policy objectives.

5.5.1 Underlying limitations: Corporate control across jurisdictions.

A critical limitation of existing data protection frameworks, including those examined in the EU and US contexts, is their implicit prioritisation of data controller interests over genuine individual autonomy. While designed to protect personal data, most contemporary regulations treat data controllers as the primary stakeholders, with individuals granted limited rights of access rather than meaningful ownership or control over their information.

This corporate-centric approach is evident across multiple jurisdictions. The GDPR, despite its rights-based rhetoric, fundamentally operates on the premise that data controllers are the legitimate custodians of personal information, with individuals granted specific enumerated rights (access, rectification, erasure) rather than comprehensive ownership.

The power asymmetry is embedded in the very definitions:

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); [...]"

(Regulation (EU) 2016/679, Art. 4(1))

"'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; [...]"

(Regulation (EU) 2016/679, Art. 4(7))

The terminology itself embeds the power relationship whereby controllers exercise control, while subjects are positioned as passive entities whose role is limited to being identified, with their agency restricted to requesting actions from controllers rather than exercising direct control over their own data. This hierarchy is consistently reinforced through request-based rights that position the controller as gatekeeper:

"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, [...]"

(Regulation (EU) 2016/679, Art. 15(1))

"The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. [...]"

(Regulation (EU) 2016/679, Art. 16)

"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay [...]"

(Regulation (EU) 2016/679, Art. 17(1))

"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller [...] and have the right to transmit those data to another controller [...]"

(Regulation (EU) 2016/679, Art. 20(1))

The regulatory text consistently positions controllers as gatekeepers through its requirement that data subjects 'obtain from the controller' access to their own information. Article 20's framing of portability rights which is applicable to data which individuals 'have provided to a controller', reveals an underlying assumption that data

ownership naturally transfers from subject to controller upon collection. Even when granting portability rights, the framework operates on the premise that controllers possess the data while individuals merely retain specific access rights.

On the other hand, the US' HIPAA's framework reflects its original purpose to facilitate insurance portability and administrative efficiency rather than patient empowerment. Enacted in 1996 to streamline transactions between healthcare providers and insurers, HIPAA treats health information as institutional data that is necessary for "treatment, payment, and healthcare operations" (45 C.F.R. § 164.506). Within this framework, patient access is structured entirely through requests to institutional gatekeepers.

"A covered entity must permit an individual to request access to inspect or obtain a copy of protected health information about the individual."

(45 C.F.R. § 164.524(a))

"An individual may request that a covered entity restrict uses or disclosures [...] A covered entity is not required to agree to a restriction"

(45 C.F.R. § 164.522(a))

This pattern mirrors GDPR. It positions patients as requestors seeking permission to view information held by institutional custodians. Individuals may request, but institutions decide. This request-based framework makes sense given HIPAA's origins, considering it was designed to facilitate data flow between institutions, with patient rights added as secondary considerations rather than core design principles.

The Malaysia's PDPA, particularly in its 2024 amendments, also reflects this paradigm. The legislation's emphasis on data controller and processor obligations, while introducing data portability rights, maintains the fundamental assumption that entities collecting data are its legitimate custodians, highlighting corporate control over personal information.

"A data subject may request the data controller to transmit his personal data to another data controller of his choice [...]"

(Act A1727, s.43A)

Even in granting portability rights, these frameworks reinforce that controllers possess the data while individuals can merely request its movement between corporate entities. The individual never achieves independent control but only the ability to petition for transfers between different controllers.

This framework becomes particularly problematic for PGHD, where individuals actively generate health data through their own devices and behaviours. Under current paradigms, the moment this self-generated data is transmitted to a platform or service

provider, individuals effectively surrender ownership rights and become supplicants requesting access to their own information. The corporate-centric model treats data subjects as beneficiaries of corporate benevolence rather than as autonomous agents with inherent rights to their personal information.

The implications for innovation and consumer autonomy are significant. When data protection laws prioritise controller interests, they inadvertently create barriers to individual-directed data sharing, limit consumer choice in service providers, and constrain the development of person-centred digital health solutions. This regulatory approach favours established institutional players while limiting opportunities for disruptive innovations that could better serve individual health management needs.

For Malaysia's PGHD governance framework, this analysis suggests the need for a fundamental paradigm shift from data protection to data ownership. Rather than granting individuals limited rights within a corporate-controlled system, effective governance should recognise individuals as the primary owners of their health data, with service providers acting as custodians subject to user-directed permissions and constraints. This ownership-based approach would better align with the principle of consumer autonomy while creating more favourable conditions for innovation in person-centred digital health services.

5.5.2 Rights-based versus innovation-driven paradigms

The European Union's approach exemplifies a rights-based paradigm that prioritises the right to protection through individual control, data sensitivity recognition, and explicit consent mechanisms. The GDPR's classification of health data as a "special category" requiring explicit consent (Article 9) creates heightened protection compared to general personal data. Combined with the EHDS's emphasis on user-controlled integration of wellness data into formal health records, this creates a framework where privacy and individual autonomy are foundational principles embedded in legal architecture. This approach places the burden on data controllers to justify processing activities and provides individuals with enforceable rights to access, portability, and deletion.

In contrast, the United States adopts an innovation-driven paradigm that emphasises the right to access and autonomy through market solutions, technological advancement, and streamlined data flows. The 21st Century Cures Act's prohibition on information blocking and mandatory API requirements for certified health IT systems reflect a policy preference for empowering individuals to direct their data flows, even when this may conflict with traditional privacy protections. The fragmented regulatory landscape with HIPAA covering institutional care but leaving consumer wearables largely unregulated creates space for rapid innovation while potentially exposing gaps in consumer protection.

These paradigmatic differences have direct implications for PGHD governance, yet they address complementary rather than competing needs. The EU model's emphasis on protection ensures comprehensive safeguards and user rights but may constrain innovation through compliance complexity and strict consent requirements. The US model's focus on access facilitates rapid technological development and user-directed data flows but creates uneven protection for consumers using health technologies outside traditional healthcare settings. Effective PGHD governance requires integrating both dimensions (protection and access) while addressing the semantic interoperability challenges that currently prevent meaningful user autonomy across vendor ecosystems.

5.5.3 Institutional coordination models

Both jurisdictions also demonstrate different approaches to institutional coordination, with significant implications for governance effectiveness. The EU's regulatory architecture reflects centralised coordination across member states, with the GDPR providing horizontal protection complemented by sector-specific regulations like the EHDS. This creates a coherent legal framework where general privacy principles are adapted to health-specific requirements while maintaining consistency across the digital economy.

The United States exemplifies decentralised coordination, where federal sectoral laws (HIPAA), federal innovation initiatives (Cures Act), and state-level privacy legislation (CCPA/CPRA) operate independently with limited integration. While this allows for policy experimentation and rapid adaptation to technological changes, it also creates compliance complexity, jurisdictional gaps, and uneven protection for consumers. Notably, this fragmentation becomes particularly problematic for PGHD, which often flows across state boundaries and between regulated (clinical) and unregulated (consumer) domains.

Malaysia's current institutional landscape more closely resembles the decentralised US model, with healthcare regulation (Ministry of Health), data protection (PDPA enforcement), and digital infrastructure (JDN/Ministry of Digital) governed by separate agencies with limited coordination mechanisms. However, Malaysia's smaller scale and more centralised government structure may provide opportunities for greater institutional alignment than is feasible in the decentralised US system. For PGHD governance specifically, this suggests Malaysia could leverage its institutional advantages to develop more coordinated approaches than currently exist in fragmented US regulatory landscape, while avoiding the potential rigidity of highly centralised systems.

5.5.4 Applicability to Malaysia's dual healthcare system

Malaysia's unique dual public-private healthcare structure creates specific challenges that neither the EU nor US models directly address. Unlike systems designed for either highly regulated environment (EU) or market-driven context (US), Malaysia must accommodate both structured government oversight and market-driven innovation within a single regulatory framework.

The EU's rights-based approach may be well-suited to Malaysia's public healthcare sector, where government oversight and standardised systems could facilitate comprehensive data protection and patient rights enforcement. The EHDS model of allowing individuals to insert wellness data into official health records, subject to explicit consent, aligns with Malaysia's MyHDW infrastructure and could support integration of PGHD into public health surveillance and clinical care delivery.

However, Malaysia's vibrant private healthcare sector, which has demonstrated greater agility in digital innovation (as discussed in Chapter 4), may benefit from elements of the US innovation-driven approach. The Cures Act's API requirements and information blocking prohibitions could encourage Malaysian private healthcare providers to adopt more open data sharing practices, potentially bridging the digital divide between public and private sectors while maintaining the innovation momentum evident in Malaysia's health technology startup ecosystem.

The CCPA/CPRA model offers particular relevance for Malaysia's PGHD governance gaps. Like California, Malaysia lacks comprehensive federal legislation specifically addressing consumer health technologies. California's approach of using horizontal privacy legislation to provide baseline protections while sector-specific frameworks are developed could inform Malaysia's strategy for managing wearable data and digital health applications that fall outside existing healthcare regulations.

5.5.5 Synthesis: Towards a hybrid model for Malaysia

The choice between rights-based and innovation-driven approaches is not merely technical but reflects deeper cultural values about privacy, autonomy, and the role of technology in society. Malaysia's cultural context, influenced by collectivist values and strong government involvement in healthcare delivery, requires a governance approach that combines the EU's structured rights protection with innovation mechanisms than with the US emphasis on market solutions and individual responsibility.

However, Malaysia's position as an upper middle-income country seeking to leverage digital technologies for healthcare advancement suggests that overly restrictive frameworks could limit innovation and economic development. The country's experience with regulatory sandboxes, its emphasis on becoming a regional digital hub, and the rapid adoption of digital health services during COVID-19 indicate strong

openness to innovation-friendly policies, provided they can be balanced with appropriate consumer protections.

This cultural context suggests that Malaysia's optimal approach may combine the EU's emphasis on structured rights protection with innovation enablement mechanisms, leveraging cultural acceptance of institutional oversight while maintaining space for the private sector innovation. The challenge lies in designing frameworks that respect collectivist values around shared responsibility and institutional trust while enabling the individual autonomy that effective PGHD governance requires.

This balance becomes particularly important given Malaysia's dual healthcare system, where public sector acceptance of government oversight must coexist with private sector demands for innovation flexibility, requiring governance frameworks that can accommodate both cultural expectations and diverse institutional needs. This hybrid approach draws selectively from both international paradigms while addressing Malaysia's unique institutional landscape.

From the EU model

Malaysia should adopt enhanced consent mechanisms that go beyond traditional opt-in/opt-out frameworks to enable granular, ongoing user control over data use. The EHDS principle of user-controlled data insertion offers a valuable template but should be expanded to recognise individuals as primary decision-makers rather than passive beneficiaries of institutional data sharing. Rights to data portability and correction should be designed to facilitate user-directed data flows rather than merely providing access to corporate-controlled information.

From the US model

Implementation of API requirements for certified health IT systems and prohibition of information blocking practices can support user autonomy by ensuring individuals can direct their data flows without institutional barriers. However, these technical capabilities should be implemented within a framework that serves individual choice rather than primarily facilitating institutional data exchange.

Addressing Malaysian specificities

The hybrid model must navigate the country's dual healthcare system by creating coordination mechanisms that respect both public sector governance requirements and private sector innovation dynamics. This requires alignment of PDPA provisions with health-specific requirements that prioritise user agency, and development of regulatory pathways for consumer health technologies that encourage innovation while ensuring meaningful user control.

This user-centric hybrid approach would require careful institutional design to manage tensions between innovation and user empowerment, public and private sector priorities, and individual autonomy and collective health benefits. By recognising individuals as primary stakeholders rather than beneficiaries of corporate data stewardship, Malaysia can create conditions for both meaningful consumer autonomy and sustainable innovation in digital health services.

5.6 Conclusion

This chapter has mapped the governance landscape for PGHD in Malaysia, revealing a complex ecosystem characterised by regulatory fragmentation, institutional silos, and significant gaps in oversight of consumer health technologies. The analysis demonstrates that while Malaysia has established comprehensive frameworks for traditional healthcare services and general data protection, the governance of PGHD from wearable devices falls into regulatory grey areas that neither healthcare-specific nor privacy-focused legislation adequately addresses.

The comparative analysis of EU and US approaches illuminates two distinct paradigms: the EU's model that emphasises individual control and data protection, versus the US innovation-driven approach prioritising interoperability and market solutions. For Malaysia, neither pure model appears fully appropriate given the country's unique dual healthcare system, cultural context, and development priorities. This suggests the need for a hybrid approach that balances consumer autonomy with innovation incentives.

The governance principles identified in this chapter which include user control, institutional coordination, and regulatory coherence, establish the foundation for technical implementation. The following chapter examines how these principles can be operationalised through data architectures and technical standards that support consumer autonomy while maintaining data quality, security, and clinical utility.

Chapter 6

Governance by design: Bridging principles and practice in the architecture of PGHD ecosystem

6.1 Introduction

The proliferation of wearable health technologies with their set of PGHD has introduced complex governance challenges. As discussed in Chapter 5, existing legal frameworks and institutional arrangements often fall short of addressing the dynamic and cross-sectoral nature of these data flows.

The absence of dedicated governance structures for PGHD especially in areas such as third-party analytics, personalised feedback delivery, and cross-border data sharing underscores the need for governance models that are not only regulatory in intent but technical in design. Rather than restricting data sharing through protective regulation, embedding user autonomy directly into system architecture can simultaneously drive innovation and enhance user protection.

This chapter responds to that gap by exploring how governance principles can be operationalised through system architecture. Rather than treating regulation and design as separate or sequential processes, this chapter adopts a “governance by design” approach by embedding legal, ethical, and policy considerations directly into the technical components of PGHD architectural design. Technical architecture thus becomes the enforcement mechanism for governance principles, making user rights actionable rather than aspirational.

This chapter explores how data management standards and protocols can be embedded into the technical components of PGHD architecture. The analysis integrates documented capabilities of existing standards with original insights into their

governance applications, focusing on how technical design can operationalise user autonomy principles. These insights subsequently inform the development of a comprehensive governance framework presented in Chapter 7.

6.2 Technical standards landscape

6.2.1 Consumer health data platforms and technical frameworks

The fundamental challenge in governing PGHD lies not merely in establishing legal frameworks, but in creating technical infrastructures that can operationalise governance principles across diverse, non-standardised data ecosystems. While existing governance literature emphasises consent, portability, and user control as essential principles, the technical reality of wearable health data reveals a critical impediment: the absence of semantic interoperability that would enable these principles to function meaningfully across platforms.

Even for seemingly universal metrics like heart rate, which is collected by virtually every consumer wearable device, there is no consistent data representation that would enable unified governance frameworks as shown in Figures 4-6 and summarised in Table 5.

This fragmentation occurs at multiple levels: schema design, field nomenclature, temporal granularity, and metadata structures. The implications extend far beyond technical inconvenience. They fundamentally constrain the implementation of user-centric governance models.

Figure 4: Google Health Connect `HeartRateRecord` schema, including fields like `startTime`, `endTime`, `samples`, and `metadata` for heart rate data representation.

```
HeartRateRecord(  
    startTime: Instant,  
    startZoneOffset: ZoneOffset?,  
    endTime: Instant,  
    endZoneOffset: ZoneOffset?,  
    samples: List<HeartRateRecord.Sample>,  
    metadata: Metadata  
)
```

Source: [Google Developer Documentation – HeartRateRecord](https://developer.android.com/reference/kotlin/androidx/health/connect/client/records/HeartRateRecord)
(Accessed from: <https://developer.android.com/reference/kotlin/androidx/health/connect/client/records/HeartRateRecord>)

Figure 5: Apple HealthKit `HKQuantitySample` schema used to represent heart rate measurements, including `quantity`, `startDate`, `endDate` and `metadata`.

```
convenience init(  
    type quantityType: HKQuantityType,  
    quantity: HKQuantity,  
    start startDate: Date,  
    end endDate: Date,  
    metadata: [String : Any]?  
)
```

Source: [Apple Developer Documentation – HKQuantitySample](https://developer.apple.com/documentation/healthkit/hkquantitysample)

(Accessed from: [https://developer.apple.com/documentation/healthkit/hkquantitysample/init\(type:quantity:start:end:metadata:\)](https://developer.apple.com/documentation/healthkit/hkquantitysample/init(type:quantity:start:end:metadata:)))

Figure 6: Samsung Health SDK `HealthConstants.HeartRate` schema fields, including heart rate value, beat count, and metadata like timestamps and device UUID.

```
{  
  "heart_rate":147.48181,  
  "heart_rate_min":99.0,  
  "heart_rate_max":124.0,  
  "start_time":1422457096536,  
  "end_time":1493922600000  
}
```

Source: [Samsung Developer Documentation – HealthConstants.HeartRate](https://developer.samsung.com/health/android/data/api-reference/com/samsung/android/sdk/healthdata/HealthConstants.HeartRate.html)

(Accessed from: <https://developer.samsung.com/health/android/data/api-reference/com/samsung/android/sdk/healthdata/HealthConstants.HeartRate.html>)

Table 5: Comparison of key heart rate data fields across different platforms (Google, Apple and Samsung)

Vendor	Dataset name	Key fields	Timestamps
Google	<code>com.google.heart_rate.bpm</code>	<code>startTime,</code> <code>endTime,</code> <code>samples,</code> <code>metadata</code>	<code>startTime,</code> <code>endTime</code>
Apple	<code>HKQuantityTypeIdentifier.heartRate</code>	<code>quantity,</code> <code>startDate,</code> <code>endDate,</code> <code>metadata</code>	<code>startDate,</code> <code>endDate</code>
Samsung	<code>HealthConstants.HeartRate</code>	<code>heart_rate,</code> <code>heart_rate_min,</code> <code>heart_rate_max,</code> <code>start_time,</code> <code>end_time</code>	<code>start_time,</code> <code>end_time</code>

Implementing user-controlled governance requires systems that can enforce granular permissions that allow users to specify precisely which types of health data can be accessed by which third parties for which purposes. When Google Health Connect represents heart rate through `HeartRateRecord` with samples arrays, Apple HealthKit uses `HKQuantitySample` with quantity values, and Samsung Health employs `heart_rate` with min/max ranges, implementing consistent consent policies becomes technically non-feasible without extensive mapping and translation layers.

This semantic fragmentation creates what can be termed "governance islands" which are isolated systems where user control mechanisms function within single platforms but cannot extend across the multi-vendor ecosystems that characterise real-world digital health usage. This occurs because vendors control their data management approaches without standardisation requirements.

6.2.2 Interoperability challenges

The cumulative effect of these technical disparities creates what can be characterised as an interoperability crisis that directly undermines governance objectives. Users generating health data across multiple devices, a smartwatch for fitness tracking, a sleep monitor for recovery analysis, and a glucose meter for metabolic health, find themselves managing fragmented data ecosystems with incompatible governance mechanisms. Each platform maintains its own consent frameworks, data access controls, and sharing permissions, creating cognitive and administrative burden that effectively constrains user autonomy.

Several technical standards have emerged to address healthcare interoperability challenges at the communication and transmission levels. However, these standards primarily address device connectivity and data transmission protocols rather than the semantic consistency and field standardisation challenges that constrain governance implementation across consumer platforms.

Legal frameworks increasingly recognise that governance principles require technical standardisation for meaningful implementation. The 21st Century Cures Act mandates API access using "successor technology" with ONC implementation rules specifically requiring HL7 FHIR-based interfaces. (146)

Similarly, GDPR's data portability rights demand "structured, commonly used and machine-readable formats" without specifying particular standards. However, these legal requirements primarily address clinical systems rather than consumer wearable ecosystems, leaving the semantic fragmentation challenges identified above largely unaddressed by regulatory mandates. (31)

HL7 FHIR (Fast Healthcare Interoperability Resources) represents a promising approach to addressing these semantic fragmentation challenges in healthcare data exchange. As a modern standard for healthcare API development, FHIR provides standardised data models and RESTful interfaces that could enable consistent data representation across consumer health platforms. However, adoption of FHIR in consumer wearable ecosystems remains limited, with most implementations focused on clinical systems rather than personal health devices. Extending FHIR standards to consumer PGHD platforms could provide the semantic consistency necessary for implementing portable user consent mechanisms and cross-platform governance frameworks, similar to how open banking standards enabled financial data interoperability. (147)

6.2.3 Authorisation and access control standards

The interoperability fragmentation identified above creates cascading challenges for access control implementation. When health data exists in semantically incompatible formats across platforms, implementing consistent authorisation policies becomes technically prohibitive. Users cannot meaningfully specify granular permissions such as "allow fitness applications to access my heart rate data for wellness tracking but not for insurance assessment" when the very definition of "heart rate data" varies across their device ecosystem.

Traditional access control models, designed for institutional environments with stable organisational hierarchies, prove inadequate for the dynamic, user-centric requirements of PGHD governance. Role-Based Access Control (RBAC) assumes predefined roles and static permission assignments that conflict with the fluid, contextual nature of personal health data sharing. Users may wish to grant temporary access to caregivers during recovery periods, provide research data to academic

studies with specific anonymisation requirements, or enable emergency access during medical crises. These scenarios that require adaptive, attribute-driven authorisation mechanisms.

The governance principle of user autonomy demands technical systems capable of operationalising fine-grained consent preferences across heterogeneous platforms and use cases. This requires access control frameworks that can capture, enforce, and audit complex user intentions while maintaining semantic consistency across the fragmented data landscape that characterises consumer health ecosystems.

OAuth 2.0 and granular consent mechanisms

OAuth 2.0 provides the foundational authorisation framework for implementing user-controlled data access in PGHD ecosystems. Unlike binary consent models that grant or deny all access, OAuth 2.0's scope mechanism enables fine-grained permissions that can specify data types, temporal boundaries, and usage purposes. For PGHD governance, this translates into user capabilities such as granting "read access to heart rate data from the last 30 days for fitness tracking purposes only."

The OAuth 2.0 authorisation code flow ensures that users maintain direct control over permission grants through explicit consent interfaces. When a health analytics application requests access to user data, the authorisation server redirects the user to a consent interface where they can review and approve specific data access requests. This user-mediated authorisation process aligns with governance principles requiring informed, explicit consent while providing the technical foundation for revocable permissions.

However, OAuth 2.0's scope mechanisms, while flexible, require standardised scope definitions to function effectively across the fragmented PGHD landscape. The semantic inconsistencies identified in Section 6.2.1 directly constrain OAuth implementation: meaningful scope definitions like "heart_rate_data" become platform-specific rather than universal, limiting the portability of user consent preferences across vendor ecosystems.

Integration with healthcare interoperability standards like HL7 FHIR could provide the semantic consistency necessary for portable OAuth scope definitions. FHIR's standardised resource types could serve as the basis for consistent scope vocabularies, enabling "heart_rate_data" to have universal meaning across platforms rather than vendor-specific interpretations.

User-Managed Access (UMA) for autonomous authorisation

User-Managed Access (UMA) 2.0 extends OAuth 2.0 to enable users to control authorisation policies for their resources without requiring constant interaction with

authorisation servers. In PGHD contexts, UMA enables users to define persistent policies such as "allow emergency contacts to access my location and vital signs during medical alerts" or "permit research institutions to access anonymised activity data for diabetes studies." (44)

UMA's policy-based approach addresses dynamic consent requirements that characterise health data sharing scenarios. Users can establish conditional access rules that respond to contextual factors: granting temporary access to caregivers during recovery periods, enabling elevated permissions during emergency situations, or allowing research access contingent on anonymisation protocols. These policies operate autonomously once established, reducing the cognitive burden of repeated authorisation decisions while maintaining user control over data access.

The UMA architecture separates resource management from authorisation policy definition, enabling users to maintain control over their data even when it resides on third-party platforms. This separation is particularly relevant for PGHD governance, where user data may be distributed across multiple cloud services, analytics platforms, and device ecosystems while still requiring consistent application of user-defined access policies.

Attribute-Based Access Control (ABAC) for contextual permissions

NIST Special Publication 800-162 defines Attribute-Based Access Control (ABAC) as a logical access control methodology that evaluates attributes of subjects, resources, actions, and environment to make authorisation decisions. For PGHD governance, ABAC provides the granular, contextual control mechanisms necessary to implement sophisticated user autonomy requirements.

ABAC policies can incorporate multiple attribute dimensions simultaneously: subject attributes (relationship to user, professional credentials, organisational affiliation), resource attributes (data sensitivity, collection context, temporal scope), action attributes (read, write, analyse, share), and environmental attributes (time of access, location, emergency status, network security level). This multi-dimensional evaluation enables complex authorisation scenarios that reflect the nuanced nature of health data sharing preferences.

Consider a scenario where a user wants to share fitness data with personal trainers but restrict access to medical monitoring data, allow broader research access during non-emergency periods but enable comprehensive access for emergency responders, and grant family members access to wellness trends but not detailed health metrics. ABAC policies can capture and enforce this complex, overlapping requirements through attribute-based rules that would be impossible to implement through role-based or simple scope-based mechanisms.

6.2.4 Security and privacy standards

The authorisation frameworks discussed in Section 6.2.3 establish the technical foundation for user-controlled access, but meaningful governance requires complementary security and privacy mechanisms that can operate effectively within the fragmented PGHD landscape. Security and privacy standards must address not only data protection during transmission and storage, but also the governance implications of data minimisation, purpose limitation, and user transparency in decentralised health ecosystems.

Data minimisation and purpose limitation in practice

Implementing governance principles such as data minimisation and purpose limitation requires technical mechanisms that can enforce these requirements throughout the data lifecycle. These represent foundational principles for privacy-preserving systems, requiring that only data necessary for specified purposes be collected, processed, or shared. In PGHD ecosystems, these principles translate into technical constraints that must be embedded within system architecture rather than enforced through external compliance mechanisms.

At the device level, data minimisation can be implemented through edge computing approaches where wearable devices perform local aggregation and filtering before transmission. A smartwatch might compute daily activity summaries, sleep quality metrics, or stress level indicators locally, transmitting only derived insights rather than granular sensor data. This approach reduces both privacy exposure and bandwidth requirements while enabling meaningful health insights.

Purpose limitation requires technical mechanisms that can enforce declared usage contexts throughout the data lifecycle. When users grant access for "fitness tracking," the system must prevent that same data from being repurposed for insurance assessment, employment screening, or commercial profiling without explicit additional consent. This enforcement requires integration between authorisation systems (discussed in Section 6.2.3) and data processing controls that can verify and audit actual usage against declared purposes.

However, implementing these principles across fragmented PGHD ecosystems faces the same semantic consistency challenges identified throughout this chapter. Without standardised definitions of data types, usage purposes, and minimisation criteria, automated enforcement becomes technically infeasible across vendor boundaries.

Encryption and data protection frameworks

ISO/IEC 27001 provides the foundational framework for information security management systems, while ISO/IEC 27701 extends these principles specifically to privacy management. (47,148) For PGHD governance, these standards establish

requirements for encryption, access logging, data retention, and incident response that must be adapted to the distributed, user-controlled nature of personal health data ecosystems.

Encryption requirements encompass both data in transit and data at rest, but PGHD ecosystems introduce additional complexity through their multi-stakeholder data flows. Health data may traverse multiple encryption domains as it flows from wearable devices to companion applications, cloud storage systems, analytics platforms, and third-party services. Each transition point represents a potential vulnerability where governance controls must be maintained alongside cryptographic protection.

End-to-end encryption approaches can preserve user control by ensuring that only authorised entities possess decryption keys, but this creates tensions with the data sharing and analytics capabilities that drive PGHD innovation. Zero-knowledge architectures which enable verification of data properties without revealing the underlying data and homomorphic encryption offer potential solutions by enabling computation on encrypted data. However, their computational overhead and implementation complexity limit current practical adoption in consumer health platforms.

The distributed nature of PGHD ecosystems also complicates key management and identity verification. Traditional public key infrastructure (PKI) assumes centralised certificate authorities, but user-controlled health data sharing may require more flexible identity and trust models that can accommodate peer-to-peer sharing, temporary access grants, and cross-platform authentication.

Zero Trust Architecture principles for PGHD

NIST Special Publication 800-207 defines Zero Trust Architecture (ZTA) as a security model that assumes no implicit trust based on network location or user credentials, requiring continuous verification of access requests. (149)For PGHD governance, Zero Trust principles align closely with user autonomy requirements by treating each data access request as a distinct authorisation decision that must be evaluated against current user preferences and contextual factors.

Zero Trust implementation in PGHD ecosystems requires treating user devices, applications, and cloud services as potentially untrusted entities that must continuously demonstrate authorisation for specific data access requests. This approach contrasts with traditional models where applications gain broad access to user health data upon initial consent, potentially enabling unauthorised secondary uses or data persistence beyond user intentions.

The "never trust, always verify" principle supports governance objectives by requiring that each data access request include verification of user consent, purpose alignment, and authorisation scope. This continuous verification model enables real-time

enforcement of user preferences, including consent revocation, purpose restrictions, and temporal limitations on data access.

Privacy-preserving computation and user transparency

Advanced privacy-preserving techniques such as differential privacy, secure multi-party computation, and federated learning offer potential solutions for enabling health data analytics while maintaining individual privacy protection. These approaches can enable population-level health insights, personalised recommendations, and clinical research without requiring centralised access to identifiable personal health data.

However, user transparency requirements demand that privacy-preserving mechanisms remain comprehensible to non-technical users. Complex cryptographic protocols and statistical privacy guarantees can become "privacy theatre" if users cannot understand or verify their protection properties. Effective governance requires transparency mechanisms that can communicate privacy protections in accessible terms while enabling meaningful user control.

6.2.5 Technical mechanisms for auditability and transparency

Building on the auditability requirements identified in Chapter 5, implementing comprehensive audit trails in distributed PGHD ecosystems requires technical mechanisms that can coordinate logging across organisational boundaries while maintaining verifiable records of data access and usage. The distributed, multi-stakeholder nature of PGHD flows creates technical challenges that extend beyond traditional centralised audit systems, requiring new approaches to log aggregation, data integrity, and cross-platform verification.

Distributed audit logging protocols

Traditional audit mechanisms assume centralised logging within single organisational boundaries, but PGHD ecosystems require coordination across wearable devices, companion applications, cloud storage systems, analytics platforms, and third-party services. Each stakeholder in the data flow may maintain separate logging systems with different formats, retention policies, and levels of detail, creating fragmentation that undermines comprehensive auditability.

Technical solutions for distributed audit logging must address several architectural challenges: ensuring consistent log formats across heterogeneous systems, maintaining temporal synchronisation across distributed components, and aggregating access records from multiple sources while preserving data integrity. Standardised logging APIs and schema definitions could enable interoperable audit

trails, though implementation requires coordination across vendor ecosystems that currently prioritise proprietary approaches.

The semantic fragmentation challenges identified throughout this chapter directly constrain audit trail implementation. When platforms use incompatible vocabularies for data types (such as demonstrated in 6.2.1), access purposes, and user relationships, creating unified audit records becomes technically prohibitive. Automated audit aggregation requires semantic consistency that remains absent from current consumer health platforms.

Cryptographic audit integrity and verification

Blockchain and distributed ledger technologies offer technical approaches for creating tamper-evident audit trails that can preserve access records across multiple stakeholders while providing cryptographic verification of log integrity. Immutable logging approaches enable verification that audit records have not been modified after creation, supporting both regulatory compliance requirements and user trust in transparency reporting.

Alternative cryptographic approaches such as hash-based audit logs and Merkle tree structures can provide tamper evidence without full blockchain implementation. These techniques enable verification of audit record integrity while potentially offering better performance characteristics for consumer health platforms.

Cross-platform audit aggregation standards

Implementing user-facing transparency across fragmented PGHD ecosystems requires technical standards for audit data exchange and aggregation. Users need unified views of their data access activities that span multiple platforms, devices, and services, but creating such interfaces requires standardised audit data formats and exchange protocols.

HL7 FHIR's `AuditEvent` resource provides a standardised schema for representing audit information in healthcare contexts, including access details, user identities, data elements accessed, and temporal information. Extending FHIR `AuditEvent` patterns to consumer wearable ecosystems could enable interoperable audit trails, though adoption requires coordination across vendor platforms that currently implement proprietary logging approaches.

OAuth 2.0 and UMA specifications include provisions for audit logging and user access to authorisation records, providing technical foundations for transparency in access control systems. However, these mechanisms focus primarily on authorisation events rather than comprehensive data usage tracking, leaving gaps in audit coverage for analytics processing, data sharing, and secondary use scenarios.

6.3 Access control in decentralised health systems

The technical standards analysis in Section 6.2 reveals a fundamental challenge. While standards exist for interoperability, authorisation, security, and audit mechanisms, their effectiveness in enabling user autonomy depends critically on how access control decisions are made and enforced across distributed PGHD ecosystems. The semantic fragmentation, vendor-specific implementations, and coordination challenges identified throughout the technical landscape directly impact the practical implementation of user-controlled data governance.

Traditional access control models, designed for centralised institutional environments, prove inadequate for the dynamic, user-centric requirements that characterise personal health data sharing. PGHD ecosystems involve multiple stakeholders with varying relationships to users, different levels of trust, and diverse usage contexts that cannot be captured through static role assignments or binary permission models. Users may need to grant temporary access to caregivers, provide conditional access for research participation, enable emergency override capabilities, or restrict certain data types while allowing others. These scenarios require sophisticated, context-aware access control mechanisms.

This section examines how access control frameworks can be designed to operationalise the governance principles established in Chapter 5 while addressing the technical constraints and interoperability challenges identified in Section 6.2. The analysis focuses on practical implementation approaches that can enable meaningful user autonomy within the current landscape of fragmented platforms and vendor-specific standards, rather than theoretical models that assume ideal technical coordination.

6.3.1 RBAC vs ABAC for PGHD environments

The choice between Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) represents a fundamental architectural decision that directly impacts the feasibility of implementing user autonomy in PGHD ecosystems. While both models provide mechanisms for controlling data access, their underlying assumptions about organisational structure, user relationships, and permission management align differently with the governance requirements identified in Chapter 5 and the technical constraints documented in Section 6.2.

Limitations of RBAC in PGHD ecosystem

RBAC operates on the principle of predefined roles within stable organisational hierarchies, where users are assigned roles that determine their access permissions. In healthcare institutions, RBAC functions effectively because roles such as "physician," "nurse," or "administrator" correspond to well-defined professional responsibilities and organisational positions. These roles remain relatively stable over time and can be centrally managed within institutional boundaries.

However, PGHD ecosystems challenge the fundamental assumptions of RBAC through their decentralised, user-centric nature. Users in PGHD systems simultaneously function as data generators, data owners, and care recipients, roles that do not map cleanly onto traditional organisational hierarchies. The relationships between users and those who may access their data such as family members, caregivers, fitness trainers, researchers and emergency responders are highly individualised and context-dependent rather than institutionally defined.

The temporal dynamics of PGHD sharing further complicate RBAC implementation. Users may need to grant temporary access during recovery periods, conditional access based on health status changes, or emergency access that bypasses normal permission structures. RBAC's static role-permission mappings cannot accommodate these dynamic requirements without constant administrative intervention, creating practical barriers to responsive user control.

Moreover, the semantic fragmentation challenges identified throughout this chapter directly constrain RBAC effectiveness. When platforms use incompatible vocabularies for user relationships and access contexts, defining consistent roles across vendor ecosystems becomes technically prohibitive. A "caregiver" role defined in one platform may not translate meaningfully to another, limiting the portability of user permission preferences.

ABAC advantages for user-controlled governance

ABAC addresses many of RBAC's limitations through its dynamic, context-sensitive approach to access decisions. Rather than relying on predefined roles, ABAC evaluates multiple attributes associated with access requests: subject attributes (user identity, relationship to data owner, credentials), resource attributes (data type, sensitivity level, collection context), action attributes (read, write, share, analyse), and environmental attributes (time, location, emergency status, network security level). (150)

This multi-dimensional evaluation enables ABAC to capture the nuanced access scenarios that characterise PGHD governance. Users can define policies such as "allow family members to access wellness trends but not detailed medical data," "permit research institutions to access anonymised activity data during non-

emergency periods," or "enable comprehensive access for emergency responders when health alerts are triggered." These complex, overlapping requirements would be impossible to implement through role-based mechanisms.

ABAC's policy-based approach also supports the dynamic consent requirements that characterise health data sharing. Users can establish conditional access rules that respond automatically to changing circumstances without requiring manual permission updates. For example, access policies can incorporate temporal constraints (30-day research participation), conditional triggers (emergency medical situations), or privacy level adjustments (anonymised vs. identifiable data sharing).

The attribute-driven nature of ABAC aligns more closely with the technical standards discussed in Section 6.2. OAuth 2.0 scopes can map directly to ABAC resource attributes, UMA policies can implement ABAC decision logic, and audit trails can capture the attribute evaluations that led to specific access decisions. This alignment enables technical implementation of sophisticated governance requirements through established standards.

6.3.2 ABAC implementation and enforcement mechanisms

While Section 6.3.1 established ABAC's conceptual advantages for PGHD governance, practical implementation requires specific technical architectures that can translate user autonomy principles into enforceable access control mechanisms. ABAC deployment in distributed PGHD ecosystems faces unique challenges that extend beyond traditional enterprise implementations, requiring solutions that can operate across vendor boundaries, accommodate mobile device constraints, and support real-time access decisions while maintaining user-comprehensible control interfaces.

User-directed policy definition mechanisms

Implementing user autonomy requires policy authoring interfaces that enable individuals to specify their access preferences without requiring technical expertise in access control languages or attribute specifications. Users need intuitive mechanisms to express preferences such as "allow family members to access wellness trends but not detailed medical data" or "permit research access to anonymised activity data during non-emergency periods" without understanding the underlying technical policy structures required for enforcement.

Template-based approaches can provide starting points for common access scenarios such as family access to wellness data, research participation with anonymisation requirements, emergency access protocols while enabling customisation for specific user needs. Policy wizards and guided configuration interfaces can help users define

complex multi-attribute rules through structured decision trees and natural language expressions rather than direct technical specification.

The challenge lies in translating user intentions into technically precise ABAC policies that can be consistently enforced across platforms. Users express preferences in contextual terms that must be mapped to specific attributes, rules, and enforcement mechanisms. This translation requires sophisticated interpretation layers that can bridge the gap between user mental models of data sharing and the technical requirements of distributed access control systems.

The semantic fragmentation challenges identified throughout this chapter directly impact the portability of user-defined policies across platforms. Access preferences defined for one vendor ecosystem may not translate meaningfully to another due to incompatible attribute vocabularies and context definitions. Standardised policy exchange formats are essential for enabling user control across fragmented vendor landscapes, though such standardisation requires coordination that extends beyond individual platform capabilities.

FHIR's resource-based architecture aligns naturally with ABAC's attribute-driven approach, where FHIR resource types could serve as standardised resource attributes, enabling consistent policy definitions across heterogeneous health platforms.

Distributed policy enforcement architecture

ABAC enforcement requires distributed policy decision and enforcement mechanisms that can operate consistently across the multi-stakeholder data flows that characterise PGHD ecosystems. The traditional Policy Enforcement Point (PEP) and Policy Decision Point (PDP) architecture must be adapted for environments where data access occurs across organisational boundaries, mobile device constraints, and real-time performance requirements.

PDP must be capable of evaluating access requests against user-defined policies while accommodating the contextual attributes that ABAC requires. This includes subject attributes (user identity, relationship credentials, trust levels), resource attributes (data sensitivity, temporal scope, anonymisation status), action attributes (read, write, analyse, share), and environmental attributes (emergency status, network security, geographic location). The computational overhead of multi-attribute evaluation must be balanced against the performance expectations of consumer health applications.

PEP require integration with the authorisation standards discussed in Section 6.2.3, particularly OAuth 2.0 and UMA mechanisms that can provide token-based access control. ABAC policies can be embedded within OAuth scopes and UMA resource

server configurations, enabling enforcement through established authorisation protocols rather than requiring entirely new access control infrastructure.

The distributed nature of PGHD flows creates challenges for policy synchronisation and consistency. When user data flows across multiple platforms and services, each enforcement point must have access to current policy definitions and attribute information. Policy distribution mechanisms must ensure that access decisions remain consistent with user preferences regardless of where data processing occurs.

Dynamic consent integration and policy updates

ABAC implementation must integrate closely with consent management systems to ensure that access control decisions align with user consent preferences and regulatory requirements. User consent directives can be translated into ABAC attributes and policy constraints, enabling automatic enforcement of purpose limitations, data minimisation requirements, and temporal consent boundaries.

Dynamic consent scenarios where users modify permissions in response to changing circumstances require policy update mechanisms that can propagate changes across distributed enforcement points in real-time. When users revoke research participation consent or modify family access permissions, all relevant PEP must receive updated policy information to prevent unauthorised access based on outdated permissions.

The integration of ABAC with audit mechanisms discussed in Section 6.2.5 enables comprehensive tracking of policy decisions and attribute evaluations. Audit trails can capture not only access events but also the specific attributes and policy rules that led to access grants or denials, supporting both regulatory compliance and user transparency about how their access control preferences are being enforced.

Performance optimisation and scalability considerations

ABAC's computational complexity creates performance challenges for consumer wearable platforms where battery life, processing power, and network connectivity need to be considered. Policy evaluation overhead must be minimised through techniques such as policy caching, attribute pre-computation, and decision memorisation that can reduce real-time evaluation requirements.

Edge computing approaches can move policy evaluation closer to data sources, reducing network latency and enabling access decisions even during connectivity disruptions. Local policy caching on wearable devices can support common access patterns while maintaining connectivity to centralised PDP for complex or infrequent access scenarios.

The scalability requirements of PGHD systems which may potentially involve millions of users each with individualised policy sets require efficient policy storage and

retrieval mechanisms. Policy indexing and optimisation strategies must enable rapid policy lookup and evaluation without creating bottlenecks that compromise user experience or system responsiveness.

6.4 Cross-sector validation: Financial services model

The governance-aware architecture principles developed throughout this chapter find validation in the financial services sector's experience with open banking initiatives. The regulatory frameworks that compelled banks to enable user-controlled data access through standardised APIs demonstrate that governance mandates can simultaneously drive innovation and enhance consumer protection. This cross-sector analysis provides empirical evidence that user autonomy over sensitive personal data, when enabled through appropriate technical standards and governance frameworks, accelerates rather than constrains innovation.

6.4.1 Malaysian digital innovation and regulatory adaptation

Malaysia's experience with fintech innovation and regulatory sandboxes provides valuable validation for the governance-by-design principles advocated throughout this chapter. The country's approach to enabling user-controlled data access through technical standards and adaptive regulatory frameworks demonstrates that governance mechanisms can simultaneously drive innovation and enhance consumer protection within sensitive data ecosystems.

Pioneering regulatory sandbox initiatives

Bank Negara Malaysia (BNM) introduced the country's first regulatory sandbox in 2016, specifically designed to enable fintech companies to operate within a controlled environment under BNM's legal framework. (151) This initiative represented a fundamental shift from restrictive regulation toward enabling innovation through adaptive governance mechanisms that could accommodate emerging technologies while maintaining consumer protection standards.

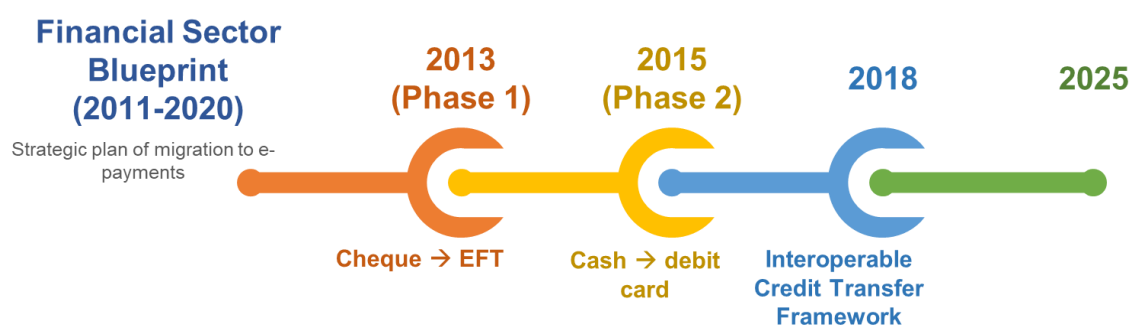
MoneyMatch became the first company to graduate from Malaysia's fintech sandbox in 2019, subsequently developing into an international fintech company providing remittance and cross-border payment services. The company also pioneered "electronic know your customer" (e-KYC) services, enabling fast customer identity authentication via mobile applications. (151) This success demonstrates that sandbox approaches can facilitate the development of innovative financial services while ensuring regulatory compliance and consumer protection.

Digital payment transformation and user autonomy

Malaysia's systematic approach to digital payment transformation demonstrates how governance frameworks can enable user control over financial data while driving technological adoption. The Financial Sector Blueprint 2011-2020 facilitated Malaysia's migration to e-payments through a phased approach that prioritised user choice and technological capability development.

The transformation occurred through three distinct phases: electronic fund transfers to displace cheques (beginning 2013), debit card adoption to displace cash (beginning 2015), and the Interoperable Credit Transfer Framework for mobile payments (beginning 2018). (152) This systematic approach enabled users to maintain control over their financial data while accessing innovative payment services, demonstrating how governance frameworks can support rather than constrain user autonomy. Figure 7 illustrates the timeline by which the financial services transformation in Malaysia took place.

Figure 7: Timeline of financial services transformation in Malaysia.



The COVID-19 pandemic accelerated digital payment adoption, with 3 million new subscribers to mobile banking services, significant increases in e-wallet usage, and 400,000 new companies adopting QR code payment systems. (153) This rapid adoption demonstrates market demand for user-controlled financial services when appropriate governance mechanisms and technical infrastructure exist to support secure, convenient access.

Cross-sector sandbox expansion

Malaysia's sandbox initiatives have expanded beyond fintech to encompass healthcare and other sectors, demonstrating the broader applicability of governance-by-design principles. The National Technology Innovation Sandbox (NTIS), led by the Ministry of Science, Technology and Innovation, operates as an interagency initiative that includes health technology hubs alongside other innovation domains.

By December 2023, NTIS had received 746 complete applications, approving 195 projects with total funding exceeding RM81 million. The program facilitated 43 regulatory cases through collaboration with 18 ministries, demonstrating the coordinated governance approach necessary for managing cross-sectoral innovation. (154) Successful health technology companies emerging from Malaysian sandboxes include digital health platforms and remote monitoring solutions that demonstrate the viability of user-controlled health data governance.

6.4.2 Open banking as governance precedent

Open banking is a financial services model that allows third party developers to access banking data and services through secure application programming interfaces. While Malaysia does not explicitly mention that they follow the open banking model, the Application Programming Interface (API) is central to the governance mechanism, similar to the United Kingdom's Open Banking Implementation Entity (OBIE) standards. (155,156) These frameworks required incumbent financial institutions to provide third-party access to customer account data through standardised APIs, contingent on explicit customer consent and strong authentication mechanisms. However, for the purpose of this thesis, data management standards and protocols outlined under the OBIE that are parallel to PGHD architecture will be discussed.

The technical implementation of open banking demonstrates how the governance principles advocated throughout this chapter can be operationalised through coordinated standards and regulatory frameworks.

6.4.3 Technical architecture parallels

The parallels between financial and health data governance are striking. Both domains involve highly sensitive personal information that users generate through their interactions with service providers. Both require sophisticated consent mechanisms that can accommodate granular permissions, temporal limitations, and purpose restrictions. Both face challenges related to data portability, cross-platform interoperability, and the need to balance innovation incentives with consumer protection requirements.

The technical implementation of open banking demonstrates how the governance principles advocated throughout this chapter can be operationalised through coordinated standards and regulatory frameworks. OAuth 2.0 serves as the foundational authorisation mechanism in both open banking and the PGHD architectures discussed in Section 6.2.3, enabling users to grant specific permissions to third-party applications without sharing their primary credentials. (157)

The open banking model employs granular scope definitions that enable users to specify precisely which account information can be accessed by which applications

for which purposes. Account Information Service Providers (AISPs) can request access to transaction history, account balances, or account details through distinct OAuth scopes, enabling users to grant partial access based on application requirements and personal preferences. This technical capability directly parallels the granular consent mechanisms required for PGHD governance, where users need to specify access to particular health data types, temporal ranges, and usage contexts.

6.4.4 Standardised data exchange formats

Open banking operations depend critically on standardised data formats and API specifications that enabled consistent implementation across diverse financial institutions. The UK's OBIE developed comprehensive technical standards that specified data schemas, API endpoints, security protocols, and message formats, eliminating the semantic fragmentation challenges that currently constrain PGHD governance.

This standardisation approach directly addresses the interoperability crisis identified in Section 6.2.1. Just as incompatible heart rate data formats across Google, Apple, and Samsung platforms prevent unified governance mechanisms, the pre-standardisation financial sector suffered from proprietary data formats that limited customer choice and third-party innovation. Open banking mandates resolved these issues through regulatory requirements for technical standardisation, demonstrating that governance frameworks can compel the coordination necessary for user autonomy.

6.4.5 Audit and transparency mechanisms

Open banking implementations include comprehensive audit requirements that parallel the transparency mechanisms discussed in Section 6.2.5. Transaction logs, access records, and consent management provide users with detailed visibility into how their financial data is being accessed and used by third-party applications. Regulatory reporting requirements ensure that both incumbent institutions and third-party providers maintain comprehensive records of data access events.

These audit mechanisms support user autonomy by enabling informed decision-making about data sharing activities. Users can review which applications have accessed their data, when access occurred, and for what declared purposes, enabling them to identify unauthorised usage and adjust their consent preferences. This transparency model provides a proven template for implementing user-facing audit capabilities in PGHD ecosystems.

6.4.6 Governance framework effectiveness

The technical and regulatory frameworks that enabled both Malaysian fintech success and open banking innovation provide validation for the governance-aware architecture principles developed throughout this chapter. Regulatory sandboxes create controlled environments where innovative data governance models can be tested and refined without compromising consumer protection. Standardised APIs eliminate the semantic fragmentation that constrains third-party innovation. OAuth 2.0 authorisation mechanisms enable granular user consent while maintaining security standards.

Importantly, both Malaysian and international experiences demonstrate that governance frameworks can be designed to enhance rather than restrict user autonomy. Rather than limiting data sharing to protect users, these regulatory approaches require incumbents to enable data sharing subject to user control. This approach aligns precisely with the governance-by-design philosophy advocated throughout this chapter, where technical architecture embeds user rights rather than constraining them through external restrictions.

6.4.7 Application to PGHD governance

The operational models of both Malaysian fintech development and international open banking provides proven models for implementing user-controlled governance in PGHD ecosystems. Malaysia's systematic approach to digital payment transformation, validated through regulatory sandboxes and cross-sector coordination, demonstrates that governance frameworks can simultaneously enhance consumer protection and accelerate innovation. This domestic experience aligns with international open banking implementations, where regulatory mandates for standardised APIs and user-controlled data access have generated rapid innovation while maintaining appropriate safeguards.

The technical architecture components such as OAuth 2.0 authorisation, standardised APIs, audit mechanisms, regulatory oversight translate directly to health data contexts. The governance principles such as user control, data portability, purpose limitation, transparency address the same user autonomy objectives that motivate PGHD governance frameworks as demonstrated in Table 6. Together, these mappings illustrate how established mechanisms in fintech governance can inform the design of more resilient and user-centric PGHD governance frameworks.

Table 6: Technical component mappings between fintech and PGHD governance frameworks

Fintech Component	PGHD Equivalent	Governance Principle
Account Information Service Provider (AISP)	Health data aggregators / analytics platforms	Third-party data access and oversight
Payment Initiation Service Provider (PISP)	Therapeutics / health interventions	User-authorised execution (based on data)
Open Banking APIs	FHIR-based health APIs	Standardised and secure data exchange
Strong Customer Authentication (SCA)	Multi-factor user authentication	Identity verification and access security
Consent dashboard (banking apps)	Health consent dashboard	User control interface
Transaction categorisation	Data type classification	Structured data organisation for purpose limitation or risk-based access
Spending insights	Personal health insights	Data analytics value

The Malaysian experience demonstrates that regulatory sandboxes can facilitate the development of health technology innovations while addressing regulatory challenges. Cross-sectoral coordination mechanisms, demonstrated through NTIS collaboration across various ministries, provide models for addressing the institutional fragmentation challenges identified in Chapter 5.

The international experience demonstrates that regulatory intervention may be necessary to compel the technical standardisation required for meaningful user autonomy. Just as open banking required standardised API schemas, healthcare interoperability demands similar coordination. HL7 FHIR provides the healthcare equivalent of open banking's data standards, though its adoption in consumer wearables lags behind clinical implementations.

The innovation outcomes observed in both contexts suggest that similar governance frameworks in health data could enable analogous benefits such as personalised health analytics, AI-powered diagnostic tools, integrated care coordination, and research applications that are currently constrained by data access restrictions. Both Malaysian and international financial sector experiences validate the central thesis of this chapter that governance-aware architectures that enable user autonomy can simultaneously drive innovation and enhance consumer protection.

This cross-sector validation reinforces the feasibility and desirability of the governance frameworks developed throughout this chapter. The technical standards, access control mechanisms, and audit requirements proposed for PGHD governance have been successfully implemented across different contexts and jurisdictions, demonstrating their practical viability. The innovation outcomes observed in financial services provide empirical evidence that user-controlled data governance can accelerate rather than constrain technological advancement, supporting the fundamental arguments underlying the governance-by-design approach advocated throughout this thesis.

6.5 Conclusion

This chapter has demonstrated that governance principles can be operationalised through technical architecture design, transforming abstract legal and policy requirements into enforceable system capabilities. The analysis reveals that the fundamental challenge in PGHD governance lies not in establishing protective regulations, but in creating technical infrastructures that embed user autonomy directly into system operation.

The semantic fragmentation analysis across major wearable platforms illustrates why current approaches fail to deliver meaningful user control. When platforms employ incompatible data schemas, even for universal metrics like heart rate, implementing consistent governance mechanisms becomes technically prohibitive. This fragmentation creates "governance islands" where user control remains trapped within vendor-specific ecosystems, undermining the cross-platform autonomy that characterises real-world digital health usage.

The technical standards examination demonstrates that existing frameworks such as OAuth 2.0, UMA, ABAC, and comprehensive audit mechanisms provide the necessary components for user-controlled data governance. However, their effectiveness depends critically on semantic standardisation that enables consistent policy enforcement across fragmented vendor landscapes. The shift from Role-Based Access Control to Attribute-Based Access Control emerges as essential for capturing the dynamic, contextual nature of personal health data sharing scenarios.

The cross-sector validation through financial services provides compelling empirical evidence that governance frameworks enabling user autonomy can accelerate rather

than constrain innovation. Open banking's success demonstrates that regulatory mandates for technical standardisation, combined with user-controlled data access mechanisms, generate rapid innovation growth while enhancing consumer protection. The systematic mapping between fintech components and PGHD equivalents shows that proven governance models can translate directly to health data contexts through established technical standards.

Importantly, this analysis validates the central thesis that governance-aware architectures can simultaneously drive innovation and enhance user protection. Rather than treating regulation and technical design as competing forces, the governance-by-design approach embeds user rights into system architecture, making compliance a natural consequence of technical operation rather than an external constraint on innovation.

The findings establish the technical feasibility of user-controlled PGHD governance while identifying semantic standardisation as the critical prerequisite for meaningful implementation. This foundation directly informs the comprehensive governance framework developed in Chapter 7, where these technical capabilities are integrated with regulatory mechanisms and institutional arrangements to create actionable pathways for transforming digital health innovation through user autonomy.

Chapter 7

Governance-by-design: A layered framework for PGHD systems

7.1 Introduction

The preceding chapters have established that the fundamental challenge in PGHD governance lies not in restricting data sharing to protect users, but in creating frameworks that embed user autonomy directly into system architecture while enabling innovation. Chapter 4 demonstrated how Malaysia's digital health ecosystem has evolved through strategic policy enablement rather than restrictive regulation. Chapter 5 revealed the fragmented governance landscape where existing frameworks constrain rather than enable user control. Chapter 6 showed that technical standards exist to operationalise user autonomy but require semantic standardisation and governance-aware implementation.

This chapter synthesises these findings into an integrated governance framework that positions user autonomy as the foundation for both consumer protection and innovation acceleration. Rather than treating governance as an external constraint on technical systems, this framework embeds user rights directly into system architecture, making compliance a part of technical operation rather than a regulatory burden.

To achieve this, the chapter first articulates the core design philosophy of governance-by-design, then presents a layered system architecture grounded in existing technical standards. This is followed by legal alignment, scenario validation, and implementation analysis to illustrate practical feasibility.

The framework addresses three critical integration challenges identified throughout this thesis: (1) aligning policy intentions with technical capabilities, (2) bridging public and private sector governance approaches, and (3) enabling user control across fragmented vendor ecosystems. By demonstrating how these challenges can be resolved through governance-aware architecture, this chapter provides actionable pathways for transforming digital health innovation through user empowerment.

7.2 Legal obligations across the PGHD lifecycle

To operationalise this framework, the first step is to align architectural principles with binding legal requirements. Accordingly, this section analyses Malaysia's PDPA 2010 (with 2024 amendments) as the reference framework, alongside the EU's GDPR as a comparative benchmark.

Other regulatory models such as HIPAA or the 21st Century Cures Act were discussed in Chapter 5 but are not examined here in order to maintain focus on frameworks most directly aligned with the design goals of the proposed architecture. These obligations form the foundation for the governance-by-design architecture developed in subsequent sections. Legal texts are often abstract; hence their obligations must be translated into concrete governance requirements. Table 7 provides this translation, outlining how rights-based provisions map to enforceable governance measures and, ultimately, to architectural design goals.

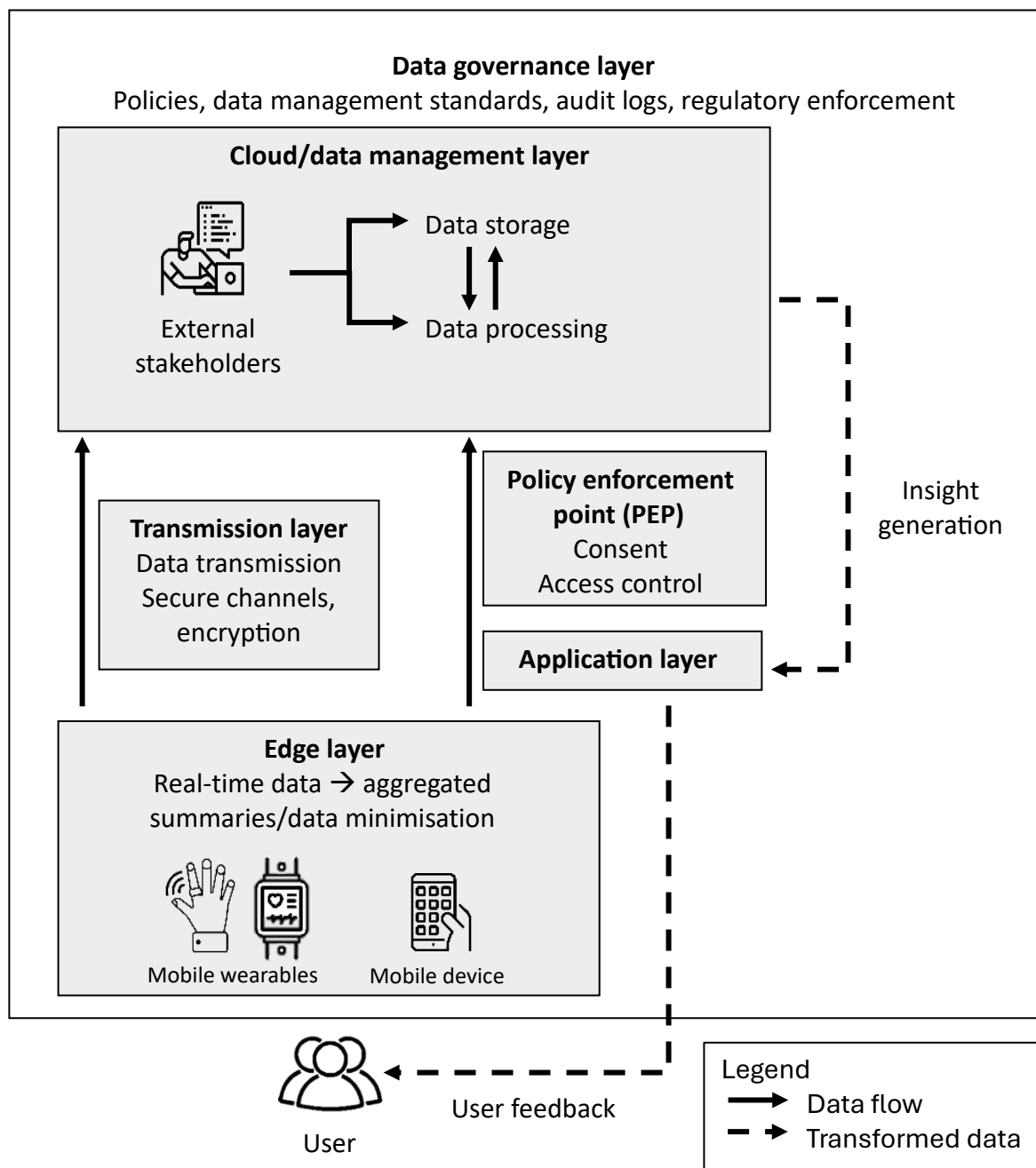
Table 7: Legal and governance alignment across the PGHD lifecycle

Lifecycle stage	Legal obligation (GDPR/PDPA)	Governance requirement
Data collection	PDPA Sec 6, GDPR Art. 6(1)(a): Consent for lawful processing	Obtain explicit and contextual consent before data collection.
Data Transmission	PDPA Sec 9, GDPR Art. 32: Secure processing and transmission	Ensure confidentiality and integrity of data during transfer through secure, encrypted channels.
Storage & Processing	PDPA Sec 10. GDPR Art. 5(1)(b) and (e): Purpose limitation and storage restriction	Restrict use to declared purposes and enforce defined retention periods.
Access & Sharing	PDPA Sec 30, GDPR Art. 15 and 20: Right to access and data portability	Enable user-directed sharing and structured data export across platforms.
Insight Delivery	PDPA Sec 7(1)(f) (transparency obligations), GDPR Art. 12 (transparency) and 22 (automated decision-making)	Ensure users can understand how insights are derived and how their data is used.

7.3 Governance-by-design: Embedding user autonomy in system architecture

To illustrate how these legal and governance requirements translate into practice, this section presents a conceptual layered data architecture for mobile health wearables. Figure 8 depicts the conceptual overview on how governance features such as consent enforcement, access control, and regulatory oversight are integrated across system layers, from edge-level data minimisation to cross-layer policy evaluation. This integrated structure ensures that user autonomy, legal compliance, and technical feasibility are maintained consistently throughout the PGHD lifecycle.

Figure 8: Conceptual layered data architecture for mobile health wearables



7.3.1 Core principles and design philosophy

The governance-by-design approach represents a fundamental paradigm shift from traditional regulatory models that impose external constraints on technical systems. Instead of treating user rights as compliance requirements to be layered onto existing architectures, this approach embeds autonomy principles directly into system design, making user control an inherent characteristic of technical operation. These principles of user ownership and semantic standardisation provide the foundation for embedding autonomy into system design. The next step is to demonstrate how they translate into enforceable architectural requirements through specific technical standards.

User ownership as architectural foundation

The framework adopts a fundamental premise that individuals are the primary owners of their health data, with service providers acting as custodians subject to user-directed permissions and constraints. This ownership-based approach contrasts sharply with the corporate-centric models identified in Chapter 5, where data controllers are treated as legitimate custodians with individuals granted limited access rights.

Under the governance-by-design model, technical architecture must recognise and enforce user ownership at every layer. Data collection, transmission, storage, processing, and sharing all operate under user-defined policies that can be modified, revoked, or transferred at user discretion. This architectural requirement transforms how systems are designed, moving from institution-centric to user-centric models of data management.

Semantic standardisation as fundamental enabler

The governance-by-design approach recognises semantic standardisation as a fundamental enabler of user autonomy. Without standardised representations for data types, usage purposes, and user relationships, sophisticated consent mechanisms remain trapped within vendor-specific ecosystems, preventing users from exercising meaningful control across their multi-platform health data ecosystem.

The framework therefore treats semantic standardisation as a governance requirement rather than a voluntary technical coordination effort. When users specify "allow fitness apps to access my heart rate data for wellness tracking but not for insurance assessment," this preference must have consistent meaning across all platforms in their ecosystem, not vendor-specific interpretations that undermine user control.

7.3.2 Governance principles to system design translation

Building on the standards analysis in Chapter 6, this section shows how governance principles can be operationalised in system design. Table 8 maps each principle to technical implementation mechanisms and relevant standards, demonstrating how autonomy, security, and accountability can be enforced at the architectural level.

Table 8: Translation of governance principles into technical architecture requirements

Governance Principle	Technical Implementation	Standards Alignment
User Consent	Fine-grained, context-aware consent frameworks using OAuth 2.0/UMA with policy engines.	OAuth 2.0, UMA 2.0
Purpose Limitation	Metadata tagging with policy enforcement through access tokens restricted by declared intent.	ABAC with purpose-aware policy evaluation
Data Portability	Structured export formats using HL7 FHIR with user-controlled APIs for platform migration.	HL7 FHIR
Transparency	Immutable audit logs with user-facing dashboards showing access patterns.	ISO 27001 audit controls
Accountability	ABAC-based accountability enforcement with breach detection.	ISO 27701
User Autonomy	User-managed interfaces enabling consent modification without administrator intervention.	UMA 2.0
Security	End-to-end encryption with Zero Trust Architecture principles.	NIST SP 800-207, ISO 27001

7.3.3 Layered architecture for governance integration

The governance-aware architecture operates across five integrated layers, each embedding specific governance controls while maintaining system performance and usability. Table 9 summarises the structure of this layered system in more detail, including the governance features implemented at each layer and their alignment with legal and technical standards. While Figure 8 provides a conceptual overview of the layers, Table 9 contains the operational breakdown of each layer.

The narrative that follows explains each layer in greater detail.

Edge layer (data minimisation)

Wearable devices implement local processing to reduce data sensitivity before transmission. Rather than streaming continuous biometric data, devices compute aggregated insights (daily activity summaries, sleep quality metrics, stress indicators) locally, transmitting only derived information necessary for specific use cases.

Transmission layer (secure transport)

All data flows employ end-to-end encryption with user-controlled key management. Zero Trust principles ensure that each transmission requires explicit authorisation verification, preventing unauthorised interception or modification during transfer.

Storage layer (distributed control)

Cloud storage systems implement user-defined retention policies with cryptographic access controls. Users specify storage duration, geographic location preferences, and access delegation rules that are technically enforced rather than contractually promised.

Application layer (purpose-aware processing)

Analytics and processing services operate under declared purposes verified through policy engines. Applications cannot repurpose data beyond stated intentions without explicit additional consent, enforced through technical constraints rather than legal agreements.

Governance overlay (cross-layer policy enforcement)

A governance layer spans all technical layers, implementing consent registries, audit trails, policy decision points, and user control interfaces that ensure consistent enforcement of user preferences across the entire data lifecycle.

Table 9: Governance-aware system architecture: Layers, features, and regulatory alignment

Layer	Description	Governance features	Legal / Standards requirements
Edge	Wearables / mobile apps	Data minimisation, local processing, consent capture	GDPR Art. 5(1)(c), GDPR Art. 25, ISO 27001.
Transmission	Secure data transport	End-to-end encryption, authorisation verification	NIST SP 800-207 Zero Trust, ISO 27001, OAuth 2.0 (RFC 6749).
Cloud	Data processing / storage	User-defined retention, access controls, geographic restrictions	GDPR Art. 20, GDPR Art. 25, ISO 27701, PDPA 2024 (data portability).
Application	Services / analytics	Purpose limitation enforcement, consent verification	GDPR Art. 5(1)(b), UMA 2.0.
Governance overlay	Cross-layer coordination	Policy evaluation, audit trails, consent registry	GDPR Art. 13-14 (transparency), NIST SP 800-162, HL7 FHIR.

7.4 Integrated data governance framework for PGHD

7.4.1. Framework architecture and core domains

The integrated data governance framework proposed in this thesis operates through four interconnected domains that embed user autonomy and legal compliance into every stage of the PGHD lifecycle. Each domain addresses a core governance challenge by aligning user rights with system design choices. Together, they form a comprehensive structure for enforceable, user-driven data control.

Domain 1: User-centric data ownership

Principle: Individuals are recognised as the primary owners of their health data, while service providers function as data custodians. This reverses the traditional model where institutions exert unilateral control over data.

Technical expression: The system architecture embeds ownership by implementing cryptographic access controls, enabling users to authorise or revoke data use without needing provider intervention.

Governance mechanisms: This domain employs user-controlled encryption keys, consent registries, portable data APIs, and revocable access tokens to enforce user-driven data control.

This domain ensures that data governance begins with the individual, transforming consent into an active control layer rather than a passive checkbox.

Domain 2: Semantic interoperability foundation

Principle: For user control to be effective across systems, data representations must be standardised to retain meaning beyond platform boundaries.

Technical expression: The framework assumes HL7 FHIR adoption for consumer health data with standardised vocabularies and relationship schemas.

Governance mechanisms: Governance is achieved through harmonised data types, purpose classifications, and user role taxonomies that enable automated, interpretable consent enforcement.

This domain provides the foundation for interoperable governance, allowing users to set preferences once and have them honoured across platforms.

Domain 3: Attribute-Based Access Control architecture

Principle: Traditional access controls rely on rigid roles. This framework adopts a more dynamic model where access decisions consider multiple contextual attributes.

Technical expression: ABAC systems are deployed to evaluate a combination of subject, resource, action, and environmental factors. This approach assumes the technical prerequisites for ABAC deployment are met.

Governance mechanisms: These include dynamic policy evaluation engines, contextual consent enforcement modules, and layered authorisation policies.

By shifting from static roles to dynamic attributes, this domain increases granularity, precision, and accountability in data governance.

Domain 4: Transparent accountability systems

Principle: Users must be able to see who accessed their data, when, and for what purpose, making transparency a governance requirement, not an afterthought.

Technical expression: The framework implements immutable audit trails integrated with user-facing transparency dashboards.

Governance mechanisms: Accountability is enforced via cryptographic logging, real-time access reporting, and decision tracking for all consent-related activities.

This domain ensures visibility and traceability across the entire data lifecycle, closing the feedback loop between consent and access.

7.4.2. Dynamic consent and authorisation mechanisms

The proposed framework moves beyond binary consent models to implement a dynamic, multidimensional approach to user authorisation. Rather than relying on opt-in or opt-out paradigms, the system captures user preferences across several axes such as data type, usage purpose, temporal scope, and recipient specificity, thus allowing granular control over personal health data.

Users can selectively permit access to specific metrics, such as heart rate or sleep patterns, and constrain usage to specific purposes such as clinical care, research, or wellness tracking. These permissions can be bound by time and recipient type, enabling highly tailored data governance.

To enforce this granularity, the framework implements attribute-based access control (ABAC), which replaces static, role-based access systems with dynamic, context-aware decision models. Access policies evaluate a combination of subject attributes (e.g., user relationship, professional affiliation), resource attributes (e.g., data sensitivity, collection context), action attributes (e.g., read, export, delete), and environmental attributes (e.g., emergency status, geographic location). This model enhances precision and accountability, ensuring that access decisions reflect real-time contextual awareness rather than predetermined user roles.

Complementing ABAC, the framework integrates User-Managed Access (UMA 2.0) protocols to delegate authorisation decisions back to the user. UMA 2.0 allows users to define persistent, conditional access rules that operate based on initial policy setup, instead of repeated authorisation for each access. This includes context-aware

policies that respond to specified environmental changes, support for trusted party delegation, and immediate revocation capabilities.

Together, these mechanisms ensure that user intent is technically enforceable, context-sensitive, and resilient across complex digital health environments.

7.4.3. Cross-platform interoperability and semantic consistency

Effective governance requires semantic consistency across heterogeneous systems. To enable meaningful user control, the framework assumes the adoption of HL7 FHIR for all consumer health data representations. This ensures that health metrics retain semantic consistency across platforms. In parallel, standardised vocabularies are applied to data types, usage purposes, user roles, and consent contexts to support interoperable policy enforcement.

Standardisation also extends to the authorisation layer, where OAuth 2.0 and UMA 2.0 APIs are used with consistent scope definitions across platforms. This guarantees that user consent preferences are intelligible and enforceable throughout the ecosystem. Additionally, audit trail schemas are harmonised to provide cross-platform transparency, allowing users to track data usage and access patterns regardless of which service provider is involved.

To ensure that user preferences persist across platform transitions, the framework introduces portable consent mechanisms. These include interoperable formats for consent representation, translation engines that map user preferences into local policy structures, and synchronisation protocols that propagate modifications in real time.

Migration support is also embedded, enabling users to transfer consent settings seamlessly when changing devices or services. Cross-platform policy coordination is achieved through technical verification and shared enforcement models based on OAuth 2.0 and UMA protocols. This ensures that consent decisions made in one part of the ecosystem remain valid and respected across others.

7.5 Governance principles integration with technical standards

7.5.1. Legal framework alignment

The integrated governance framework proposed in this thesis is designed to align directly with enforceable rights and obligations under both the EU GDPR and Malaysia's PDPA, including its 2024 amendments. Rather than treating legal compliance as a post-hoc function or external audit requirement, the architecture embeds these obligations within the system's core design, enabling automated, user-centric enforcement.

In the context of the GDPR, several key principles are operationalised at the architectural level. Article 6 establishes lawful grounds for processing personal data,

while Article 9 requires explicit consent specifically for processing health-related data. These requirements are addressed through OAuth 2.0 and UMA 2.0 protocols that enable dynamic, fine-grained consent tied to specific data types, usage purposes, and recipient categories. Rather than relying on static checkboxes or institutional forms, consent becomes an executable policy enforced through authorisation flows that directly reflect user intent.

The framework also addresses the GDPR's purpose limitation principle (Article 5(1)(b)) and storage limitation principle (Article 5(1)(e)) by implementing metadata tagging and purpose-binding at the point of data collection. These design elements ensure that data is only used for its declared purpose and retained only as long as necessary, consistent with the regulation's expectations. Data portability under Article 20 is supported through HL7 FHIR-compliant export capabilities, allowing structured and interoperable data transfer between services.

From a Malaysian legal perspective, the framework incorporates the updated provisions of the PDPA 2024, particularly those concerning consent, access rights, and security obligations. Section 6 of the PDPA, which requires consent prior to data processing, is enforced through the same authorisation infrastructure described above. Section 30, which outlines the right to access personal data, is operationalised via user dashboards and data retrieval APIs that ensure timely and secure access. The 2024 amendment's inclusion of processor obligations under the security principle is addressed through distributed enforcement models and audit logging.

In both jurisdictions, the proposed architecture reframes legal compliance as a function of system behaviour rather than institutional promise. This governance-by-design approach reduces reliance on external enforcement mechanisms by making non-compliant data use technically infeasible, thus raising the baseline for trustworthy health data ecosystems.

7.5.2. Technical standards synthesis

The technical foundation of the proposed governance framework builds on three key standards families: OAuth 2.0 and UMA for access control, Zero Trust principles for contextual verification, and HL7 FHIR for semantic interoperability.

OAuth 2.0 and UMA 2.0 serve as the core authorisation infrastructure, enabling users to exercise granular control over who can access their health data, for what purpose, and under what conditions. By extending beyond basic OAuth scopes, the framework implements health-specific scope definitions that capture real-world data sharing scenarios. Users can grant permissions such as "read access to heart rate data from the last 30 days for fitness tracking purposes only," with technical enforcement through token-based mechanisms.

UMA 2.0 further enhances this capability by allowing users to define sophisticated, persistent authorisation policies, including conditional rules and delegated access. These protocols ensure that user intent is captured and enforced directly through authorisation flows rather than relying on institutional compliance promises.

In parallel, the architecture adopts Zero Trust principles to reinforce secure and context-aware access. Each data access request is evaluated in real time, incorporating environmental and behavioural factors such as device context, network integrity, and geographic location. This “never trust, always verify” model replaces static credentials with continuous risk-based authorisation, thereby enforcing minimal privilege and limiting access to only the data necessary for the declared use.

Lastly, HL7 FHIR standards are used to achieve interoperability and data portability across diverse platforms. The framework assumes FHIR resource-based models to represent consumer health metrics in a structured and extensible manner. Consistent RESTful APIs ensure predictable behaviour across systems, while FHIR’s extensibility mechanisms allow the architecture to evolve in tandem with emerging health data types and analytics requirements. These technical standards work in concert to translate governance goals into enforceable system behaviour.

7.6 Framework validation through hypothetical scenario

To illustrate how the proposed governance framework operates in practice, this section presents a hypothetical real-world use case involving post-operative recovery monitoring through wearable devices. The scenario assumes the availability of technical capabilities described throughout this thesis framework, including seamless cross-platform interoperability and standardised policy exchange protocols. While these capabilities require further development in current systems, the scenario demonstrates how governance principles would operate when embedded in technical architecture.

7.6.1 Scenario walkthrough

The scenario follows Bob, a patient recovering from surgery, who uses a smartwatch to track key health metrics while retaining granular control over how his data is accessed and used.

Bob’s smartwatch collects heart rate, blood pressure, step count, and sleep quality data to support his recovery at home. Rather than transmitting continuous raw data, the device locally aggregates readings into daily health summaries. It also applies differential privacy techniques to protect sensitive activity patterns while maintaining clinically relevant signals. This approach aligns with the framework’s edge layer implementation for data minimisation.

Using the smartwatch's companion mobile application, Bob configures detailed consent preferences to reflect the varying roles of stakeholders involved in his care. His surgeon is granted full access to biometric data for a six-week post-operative period. His physiotherapist is allowed to view activity summaries for 12 weeks to support rehabilitation.

Emergency contacts are authorised to view vital signs only during predefined alert conditions, while an anonymised subset of his data is shared with a research database to contribute to surgical outcome studies. These consent settings reflect the framework's support for purpose-specific and context-aware data sharing.

When Bob's surgeon attempts to access his heart rate data, the system triggers an ABAC evaluation. The policy engine assesses multiple dimensions: the requester is a verified healthcare provider with a pre-established patient relationship; the requested resource is biometric data collected within the relevant post-surgical window; the intended action is clinical review; and the environmental context includes access during normal working hours on a secure network. The request is granted because it aligns with Bob's configured consent rules.

Each access event generates an immutable audit trail that logs the requester's identity, credentials, the specific data accessed, the stated purpose, and the duration of access. This audit log is cross-referenced with Bob's consent preferences and is made available for user inspection through a transparency dashboard. Bob can review all access events, ensuring full visibility into how, when, and why his data is being used.

When Bob decides to replace his smartwatch with a newer model from a different manufacturer, his consent preferences are automatically transferred using standardised policy exchange protocols. The new device honours his existing authorisation settings without requiring reconfiguration, demonstrating how cross-platform interoperability and portable consent mechanisms are achieved through governance-aware system design.

This walkthrough demonstrates how governance-by-design enables both flexibility and accountability in personal health data management. The system enforces user-defined policies dynamically and transparently, ensuring continuity of care without compromising user autonomy or data protection.

7.6.2 Technical architecture validation

The scenario outlined in the previous section serves as a validation of the proposed governance framework by demonstrating how abstract governance principles can be operationalised through concrete technical mechanisms.

First, it exemplifies user autonomy by enabling Bob to exercise granular control over who accesses his health data, for what purpose, and under which conditions. This

fine-grained consent model supports a patient-centric governance paradigm, moving beyond static permission forms to dynamic, enforceable user intent.

Second, the framework enforces purpose limitation through policy engines that condition access on context-specific attributes. Bob's healthcare providers are technically constrained to only access data aligned with the declared clinical objectives, ensuring compliance with legal and ethical data minimisation principles.

Third, the system fosters transparency by maintaining immutable audit trails that record all access events in a user-visible manner. This not only deters misuse but also enables Bob to monitor and verify compliance with agreed terms.

Finally, the framework demonstrates data portability by enabling seamless migration of consent policies when Bob switches devices. The preservation of user preferences across vendor ecosystems validates the feasibility of interoperable, standard-based policy exchange.

In addition to governance principles, the scenario confirms the operational viability of the technical standards proposed in Chapter 6. OAuth 2.0 and UMA 2.0 protocols enable user-controlled authorisation flows that enforce consent dynamically. The use of HL7 FHIR ensures that health data retains semantic consistency across platforms, enabling cross-vendor interoperability. ABAC facilitates context-sensitive decision-making that reflects real-world healthcare needs. Finally, the framework's use of Zero Trust Architecture principles ensures that access is continuously verified, with each request evaluated against current user consent policies and contextual risk factors.

Together, these components validate the feasibility of governance-by-design for PGHD ecosystems and illustrate how trust, autonomy, and innovation can be technically harmonised.

7.7 Conclusion

This final section consolidates the architectural, legal, and institutional insights developed throughout the chapter and reflects on their broader implications for digital health governance. This thesis has demonstrated that user autonomy and technological innovation are not mutually exclusive but can be mutually reinforcing each other when embedded directly into system architecture. By treating governance not as an external constraint but as a core design principle, the proposed framework shows how individual control can drive, rather than restrict responsible innovation in digital health.

The synthesis of regulatory insights and technical standards outlined in Chapters 5 and 6 reveals that the core capabilities needed for governance-aware systems already exist. Standards such as OAuth 2.0, HL7 FHIR, UMA 2.0, and ABAC provide the technical foundation for dynamic consent, granular access control, and interoperable policy enforcement. The key challenge lies not in technical feasibility, but in achieving

semantic consistency and cross-platform alignment across fragmented vendor ecosystems.

Empirical validation from Malaysia's fintech sector further supports this governance model. As shown in Chapter 5, the success of open banking initiatives demonstrates that frameworks enabling user-directed data sharing can accelerate innovation, build public trust, and align with local institutional and cultural norms. These findings reinforce the potential for similar governance-by-design strategies to succeed in Malaysia's digital health context.

Critically, the framework recognises that long-term digital health innovation requires more than regulatory compliance. It demands genuine user trust and engagement. When autonomy is embedded at the architectural level, compliance with user preferences becomes a built-in system function, not a discretionary policy. This marks a shift from governance as institutional oversight to governance as system behaviour.

By reframing governance in this way, the framework proposes more than incremental reform. It reimagines the foundations of digital health by prioritising user empowerment, transparency, and interoperability. In an age where digital platforms increasingly shape access to health, wellbeing, and opportunity, meaningful user control over personal data must be recognised as a prerequisite for equitable participation in the digital economy.

However, realising this potential depends not only on technical architecture but also on institutional alignment. A central coordinating authority, whether national, regional, or sectoral, will be essential to ensure the consistent adoption of shared standards such as HL7 FHIR and UMA. Without such coordination, the architecture's benefits risk being diluted by inconsistent implementation across siloed platforms.

Chapter 8

Discussion and contributions

8.1. Implementation challenges and governance integration

While the proposed governance framework demonstrates technical feasibility and conceptual coherence, its real-world implementation in consumer-facing PGHD ecosystems encounters substantial challenges. This section discusses critical obstacles to adoption, focusing on limitations in existing platforms, semantic standardisation issues, and architectural complexity.

8.1.1 Device constraints and experience trade-offs

Mobile health wearables typically operate under significant hardware constraints, such as limited processing power, battery life, and screen size. These constraints restrict the deployment of complex authorisation protocols like ABAC and UMA 2.0, which require real-time policy evaluation and dynamic consent enforcement. Vendors prioritise simplified user experiences such as all-or-nothing data sharing toggles over granular, user-controlled authorisation flows. As a result, the governance principles outlined in Chapter 7 may remain technically infeasible or commercially unattractive without further advances in low-overhead policy engines and UI abstraction layers.

8.1.2 Semantic fragmentation and interoperability barriers

Effective implementation of ABAC and dynamic consent frameworks requires shared vocabularies for data types, usage purposes, and user roles. However, current wearable ecosystems remain deeply fragmented, with platform-specific interpretations of health data semantics. This undermines cross-platform policy portability, a key enabler of user autonomy. As highlighted in Section 6.2, semantic standardisation (e.g. HL7 FHIR, OAuth scope harmonisation) is not merely a technical requirement but a governance prerequisite. Without consistent definitions, even technically sound architectures fail to deliver enforceable user control.

8.1.3 Security integration and Zero Trust Tensions

The Zero Trust Architecture (ZTA) model proposed in Chapter 6 ensures continuous authentication and contextual access verification, aligning well with governance goals. However, ZTA's security overhead may degrade user experience in consumer settings, where frictionless access is expected. Additionally, enforcing Zero Trust across fragmented systems with varied capabilities can lead to inconsistent implementations. Balancing rigorous enforcement with usability remains a key design tension.

8.2. Hybrid access control models

While ABAC offers superior granularity and contextual precision, its implementation complexity and semantic dependencies pose usability challenges. A hybrid approach that layers ABAC over RBAC may provide a viable compromise. Role templates (e.g. family member, emergency provider) can simplify user interaction, while allowing attribute-based refinement for advanced scenarios. This preserves accessibility without sacrificing governance precision.

8.3. Standardisation as a coordinating mechanism

Governance-by-design cannot be achieved through technical innovation alone. Institutional coordination is essential. A central authority such as a national standards body, sectoral regulator, or designated health data agency must drive the adoption of shared vocabularies, interface protocols, and policy exchange formats. As shown in the open banking case from Chapter 5, regulatory mandates can catalyse ecosystem-wide alignment, overcoming commercial incentives for vendor lock-in. HL7 FHIR and UMA 2.0 are only effective if mandated and adopted by ecosystem-wide coordinating authorities.

8.4. Contributions to theory and practice

This research contributes to digital health governance scholarship and practice across three interconnected domains:

8.4.1. Theoretical innovation:

The thesis introduces governance-by-design as an architectural paradigm where user autonomy is embedded directly into technical system design rather than imposed through external regulatory requirement. This approach transforms legal compliance from a post-hoc requirement into a foundational design principle. By demonstrating how user rights can be operationalised through system architecture, the research shifts the discourse from institutional oversight toward user empowerment, bridging a long-standing divide in health informatics scholarship.

8.4.2. Technical integration

The framework provides a systematic synthesis of data standards such as OAuth 2.0, UMA 2.0, HL7 FHIR, and ABAC to create enforceable user-centric governance mechanisms for PGHD ecosystems. This integration addresses the semantic fragmentation across vendor platforms and demonstrates how established standards can be coordinated to enable dynamic consent, purpose limitation, and cross-platform policy enforcement. In doing so, it translates abstract governance principles into implementable technical specifications that can be validated in practice.

8.4.3. Policy validation

Through cross-sector analysis, the thesis provides empirical evidence that user-controlled data frameworks can accelerate innovation while safeguarding consumer protection. The comparative study of Malaysian fintech governance and international open banking illustrates that governance-enabling approaches need not limit technological progress but can, in fact, drive it. This policy-oriented validation challenges prevailing assumptions that data protection and innovation are inherently in conflict, offering instead a model where they can be mutually reinforcing.

Taken together, these contributions offer a reference framework for jurisdictions with dual healthcare systems and fragmented vendor ecosystems. Its applicability extends to contexts where semantic interoperability limits user control and where institutional coordination is required to enable consistent, cross-platform governance.

Chapter 9

Conclusion

This thesis addressed a fundamental challenge in digital health governance whereby existing frameworks constrain rather than enable user autonomy over PGHD, thus limiting both individual empowerment and innovation potential. Through analysis of Malaysia's digital health evolution, comparative examination of international governance approaches, and technical evaluation of existing standards, this research demonstrates that the solution requires embedding user control directly into system architecture rather than imposing external regulatory constraints.

The research makes three core contributions to digital governance scholarship. First, it introduces the governance-by-design paradigm that shifts from data protection through restriction to user empowerment through embedded technical capabilities, treating user autonomy as an architectural requirement rather than a compliance afterthought. Second, it develops a multi-domain integration framework that systematically bridges policy analysis, legal review, and technical implementation to create governance solutions that are simultaneously policy-informed, legally coherent, and technically feasible. Third, it provides empirical insights demonstrating that enabling governance approaches can accelerate innovation while maintaining consumer protection, validated through Malaysia's dual-sector digital health evolution and cross-sector comparison with financial services governance models.

The research identifies semantic standardisation as the critical prerequisite for meaningful user autonomy across fragmented vendor ecosystems and demonstrates how existing technical standards (OAuth 2.0, HL7 FHIR, ABAC) can be integrated to enable user-controlled governance when coordinated implementation occurs across platforms. Cross-sector validation through open banking provides compelling empirical evidence that user-controlled data frameworks accelerate rather than constrain innovation when implemented with appropriate technical standards and regulatory coordination.

While the framework demonstrates theoretical and technical feasibility, it requires empirical validation through pilot implementations and user experience studies. Future research should examine collective governance integration, cross-domain applications, and long-term innovation impact assessment to validate the framework's broader applicability and effectiveness.

This research demonstrates that sustainable digital health innovation requires user trust achievable only through genuine control over personal health data. By embedding autonomy into technical architecture, governance-by-design approaches can transform digital health governance from an innovation barrier into an enabler, creating conditions where individual rights and technological advancement become mutually reinforcing objectives.

The vision underpinning this research can be summarised as follows: In an era where digital health technologies play an increasingly important role in improving health outcomes, empowering individuals with meaningful control over their health data is not only a matter of safeguarding privacy rights, but also a fundamental prerequisite for a sustainable digital health transformation.

Abbreviations

4IR	Fourth Industrial Revolution
ABAC	Attribute-Based Access Control
AI	Artificial Intelligence
AISP	Account Information Service Provider
API	Application Programming Interface
AWS	Amazon Web Services
BNM	Bank Negara Malaysia
CCPA	California Consumer Privacy Act
CIS	Clinical Information System
CME	Continuing Medical Education
CPRA	California Privacy Rights Act
DPO	Data Protection Officers
e-KYC	Electronic Know Your Customer
EHDS	European Health Data Space
EHl	Electronic Health Information
EHR	Electronic Health Records
EMR	Electronic Medical Records
EU	European Union
FAIR	Findable, Accessible, Interoperable, Reusable
FDA	U.S. Food and Drug Administration
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation

GIS	Geographic Information System
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HL7	Health Level 7
ICT	Information and Communication Technology
IoT	Internet of Things
JDN	Jabatan Digital Negara (National Digital Department)
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit
MCMC	Malaysian Communications and Multimedia Commission
MDA	Medical Device Authority
MHTC	Malaysia Healthcare Travel Council
MoH	Ministry of Health
MRANTI	Malaysian Research Accelerator for Technology and Innovation
MyHDW	Malaysian Health Data Warehouse
NIST	National Institute of Standards and Technology
NKEA	National Key Economic Areas
NPRA	National Pharmaceutical Regulatory Agency
NRS	National Regulatory Sandbox
NTIS	National Technology Innovation Sandbox
OAuth	Open Authorization
OBIE	Open Banking Implementation Entity
ONC	Office of the National Coordinator for Health Information Technology
OOP	Out-of-Pocket
PDPA	Personal Data Protection Act
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PGHD	Patient-Generated Health Data

PISP	Payment Initiation Service Provider
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
SCA	Strong Customer Authentication
THIS	Total Hospital Information System
UK	United Kingdom
UMA	User-Managed Access
US	United States
ZTA	Zero Trust Architecture

Bibliography

1. Chen X, Kim DH, Lu N. Introduction: Wearable Devices [Internet]. Vol. 124, Chemical Reviews. American Chemical Society; 2024 [cited 2025 Jan 5]. p. 6145–7. Available from: <https://doi.org/10.1021/acs.chemrev.4c00271>
2. Kang HS, Exworthy M. Wearing the Future—Wearables to Empower Users to Take Greater Responsibility for Their Health and Care: Scoping Review. JMIR Mhealth Uhealth [Internet]. 2022 Jul 13 [cited 2025 Jan 5];10(7):e35684. Available from: <https://mhealth.jmir.org/2022/7/e35684>
3. Jackson MEJ, Bernstein SW, Werling K. Digital_Health_Investing_in_2023. Medical Product Outsourcing [Internet]. 2023 Oct [cited 2025 Jan 6];21(8). Available from: <https://www.mpo-mag.com/digital-health-investing-in-2023-seizing-opportunity-amid-slower-investment-landscape/>
4. Zakerabasali S, Ayyoubzadeh SM, Baniyadi T, Yazdani A, Abhari S. Mobile health technology and healthcare providers: Systemic barriers to adoption. Healthc Inform Res [Internet]. 2021 Oct 1 [cited 2025 Jan 6];27(4):267–78. Available from: <https://synapse.koreamed.org/articles/1147966>
5. Osama M, Ateya AA, Sayed MS, Hammad M, Pławiak P, Abd El-Latif AA, et al. Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. Vol. 23, Sensors. Multidisciplinary Digital Publishing Institute (MDPI); 2023.
6. Suleiman TA, Adinoyi A. Telemedicine and Smart Healthcare—The Role of Artificial Intelligence, 5G, Cloud Services, and Other Enabling Technologies. International Journal of Communications, Network and System Sciences. 2023;16(03):31–51.
7. Grys CA. Digital health: The next evolution of healthcare delivery. Nursing (Brux). 2022 Oct;52(10).
8. Willems SH, Rao J, Bhambere S, Patel D, Biggins Y, Guite JW. Digital solutions to alleviate the burden on health systems during a public health care crisis: Covid-

- 19 as an opportunity. Vol. 9, JMIR mHealth and uHealth. JMIR Publications Inc.; 2021.
9. Khatiwada P, Yang B, Lin JC, Blobel B. Patient-Generated Health Data (PGHD): Understanding, Requirements, Challenges, and Existing Techniques for Data Security and Privacy. Vol. 14, Journal of Personalized Medicine. Multidisciplinary Digital Publishing Institute (MDPI); 2024.
 10. Kawu AA, Hederman L, Doyle J, O’Sullivan D. Patient generated health data and electronic health record integration, governance and socio-technical issues: A narrative review. Vol. 37, Informatics in Medicine Unlocked. Elsevier Ltd; 2023.
 11. European Union. Regulation (EU) 2025/327 (European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847). Official Journal of the European Union, L 327. Mar, 2025 p. 1–127.
 12. United States Congress. 21st Century Cures Act [Internet]. U.S. Government Publishing Office, 114–255 United States: U.S. Food and Drug Administration; Dec, 2016. Available from: <https://www.fda.gov/regulatory-information/selected-amendments-fdc-act/21st-century-cures-act>
 13. Torab-Miandoab A, Samad-Soltani T, Jodati A, Akbarzadeh F, Rezaei-Hachesu P. A unified component-based data-driven framework to support interoperability in the healthcare systems. Heliyon. 2024 Aug 15;10(15).
 14. Cortez A, Hsui P, Mitchell E, Riehl V, Smith P. Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024 [Internet]. 2018 [cited 2025 Jul 4]. Available from: https://www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf?utm_source=chatgpt.com
 15. Ravidas S, Lekidis A, Paci F, Zannone N. Access control in Internet-of-Things: A survey. Journal of Network and Computer Applications. 2019 Oct 15;144:79–101.
 16. Gazzarata R, Almeida J, Lindsköld L, Cangioli G, Gaeta E, Fico G, et al. HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in digital healthcare ecosystems for chronic disease management: Scoping review. Vol. 189, International Journal of Medical Informatics. Elsevier Ireland Ltd; 2024.
 17. Kawu AA, O’Sullivan D, Hederman L. Towards Exchanging Wearable-PGHD with EHRs: Developing A Standardized Information Model for Wearable-Based Patient Generated Health Data. Proceedings of the Sixteenth International Conference on Advances in Semantic Processing (SEMAPRO 2022) [Internet]. 2022 Sep; Available from: <https://www.researchgate.net/publication/363783802>

18. Abraham R, Schneider J, vom Brocke J. Data governance: A conceptual framework, structured review, and research agenda. Vol. 49, *International Journal of Information Management*. Elsevier Ltd; 2019. p. 424–38.
19. Micheli M, Ponti M, Craglia M, Berti Suman A. Emerging models of data governance in the age of datafication. *Big Data Soc*. 2020 Jul 1;7(2).
20. Weber K, Otto B, Österle H. One size does not fit all -A contingency approach to data governance. *Journal of Data and Information Quality*. 2009;1(1).
21. Khatri V, Brown C V. Designing data governance. *Commun ACM*. 2010 Jan 1;53(1):148–52.
22. Janssen M, Brous P, Estevez E, Barbosa LS, Janowski T. Data governance: Organizing data for trustworthy Artificial Intelligence. *Gov Inf Q*. 2020 Jul 1;37(3).
23. Wilkinson MD, Dumontier M, Aalbersberg IJ, Appleton G, Axton M, Baak A, et al. Comment: The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data*. 2016 Mar 15;3.
24. Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in health care. Vol. 27, *Journal of the American Medical Informatics Association*. Oxford University Press; 2020. p. 491–7.
25. Winter JS. AI in healthcare: Data governance challenges. Vol. 5, *Journal of Hospital Management and Health Policy*. AME Publishing Company; 2021.
26. Greenhalgh T, Wherton J, Papoutsis C, Lynch J, Hughes G, A’Court C, et al. Beyond adoption: A new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the scale-up, spread, and sustainability of health and care technologies. *J Med Internet Res*. 2017 Nov 1;19(11).
27. Sharon T. Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. *Philos Technol*. 2017 Mar 1;30(1):93–121.
28. Van Kleek M, Liccardi I, Binns R, Zhao J, Weitzner DJ, Shadbolt N. Better the devil you know: Exposing the data sharing practices of smartphone apps. In: *Conference on Human Factors in Computing Systems - Proceedings*. Association for Computing Machinery; 2017. p. 5208–20.
29. Hummel P, Braun M, Dabrock P. Own Data? Ethical Reflections on Data Ownership. *Philos Technol*. 2021 Sep 1;34(3):545–72.
30. Purtova N. TILBURG LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency [Internet]. Available from:

<http://ssrn.com/abstract=3070228>Electronic copy available at: <https://ssrn.com/abstract=3070228>

31. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119. 2016 p. 1–88.
32. McDonald AM, Cranor LF. Database Nation: The Death of Privacy in the 21st Century [Internet]. 2001. Available from: <http://www.is-journal.org/>
33. Solove DJ. PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA. Harv Law Rev. 2013;126:18801903.
34. Mikalef P, Boura M, Lekakos G, Krogstie J. The role of information governance in big data analytics driven innovation. Information and Management. 2020 Nov 1;57(7).
35. Lane J, Stodden V, Bender S, Nissenbaum H. Privacy, big data, and the public good: Frameworks for engagement. Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge University Press; 2013. 1–322 p.
36. Dimitrov D V. Medical internet of things and big data in healthcare. Vol. 22, Healthcare Informatics Research. Korean Society of Medical Informatics; 2016. p. 156–63.
37. Hripcsak G, Bloomrosen M, Flatley Brennan P, Chute CG, Cimino J, Detmer DE, et al. Health data use, stewardship, and governance: Ongoing gaps and challenges: A report from AMIA's 2012 health policy meeting. Journal of the American Medical Informatics Association. 2014;21(2):204–11.
38. Rosenbaum S. Data governance and stewardship: Designing data stewardship entities and advancing data access. Vol. 45, Health Services Research. 2010. p. 1442–55.
39. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: A patient interface for twenty-first century research networks. European Journal of Human Genetics. 2015 Feb 20;23(2):141–6.
40. Kostkova P, Brewer H, de Lusignan S, Fottrell E, Goldacre B, Hart G, et al. Who Owns the Data? Open Data for Healthcare. Front Public Health. 2016 Feb 17;4.
41. Richards N, Hartzog W, Baker S, Citron D, Heusel J, King J, et al. THE PATHOLOGIES OF DIGITAL CONSENT.
42. Budin-Ljøsne I, Teare HJA, Kaye J, Beck S, Bentzen HB, Caenazzo L, et al. Dynamic Consent: A potential solution to some of the challenges of modern biomedical research. BMC Med Ethics. 2017 Jan 25;18(1).

43. Lehtiniemi T, Kortensniemi Y. Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data Soc.* 2017 Dec 1;4(2).
44. Kantara Initiative. User-Managed Access (UMA) Profile of OAuth 2.0 [Internet]. 2015 Dec [cited 2025 Jul 5]. Available from: <https://docs.kantarainitiative.org/uma/rec-uma-core.html>
45. Cavoukian A. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices [Internet]. 2011 [cited 2025 Jul 5]. Available from: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>
46. Zuboff S. Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum.* 2019 Jan 1;28(1):10–29.
47. International Organization for Standardization; International Electrotechnical Commission. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva, Switzerland; 2022 Oct.
48. Ioannidou I, Sklavos N. On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. *Cryptography.* 2021 Dec 1;5(4).
49. Mone V, Shakhlo F. Health Data on the Go: Navigating Privacy Concerns with Wearable Technologies. *Legal Information Management.* 2023 Sep;23(3):179–88.
50. Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Vol. 153, *Computer Communications.* Elsevier B.V.; 2020. p. 311–35.
51. Viceconti M, Hunter P, Hose R. Big Data, Big Knowledge: Big Data for Personalized Healthcare. *IEEE J Biomed Health Inform.* 2015 Jul 1;19(4):1209–15.
52. Hevner AR, March ST, Park J, Ram S. DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1. Vol. 28, *Design Science in IS Research MIS Quarterly.* 2004.
53. Creswell JW, Poth CN. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* 5th ed. SAGE Publications; 2018.
54. Yin RK. *Case Study Research and Applications: Design and Methods.* 6th ed. SAGE Publications; 2018.
55. Bowen GA. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal.* 2009 Aug;

56. Jaafar S, Mohd Noh K, Abdul Muttalib K, Othman NH, Healy J. Malaysia Health System Review. Healy J, editor. Vol. 3. World Health Organisation; 2013.
57. Health Informatics Centre. 2023 Health Facts (Reference Data for Year 2022). Ministry of Health Malaysia; 2023.
58. Malaysia National Health Accounts Section. Malaysia National Health Account Health Expenditure Report 2011-2021. Ministry of Health Malaysia; 2023.
59. Sayuti M, Sukeri S. Assessing progress towards Sustainable Development Goal 3.8.2 and determinants of catastrophic health expenditures in Malaysia. PLoS One. 2022 Feb 1;17(2 February).
60. Anis-Syakira J, Jawahir S, Abu Bakar NS, Mohd Noh SN, Jamalul-Lail NI, Hamidi N, et al. Factors Affecting the Use of Private Outpatient Services among the Adult Population in Malaysia. Int J Environ Res Public Health. 2022 Oct 1;19(20).
61. Tew MM, Hatah E, Arif F, Abdul Wahid MA, Makmor-Bakry M, Abdul Maulad KN. Geospatial analysis of distribution of community pharmacies and other health care facilities providing minor ailments services in Malaysia. J Pharm Policy Pract. 2021 Dec 1;14(1).
62. PwC Malaysia. Healthcare in a Digital Economy: Reimagining the Future of HealthTech in Malaysia [Internet]. 2021 Nov [cited 2025 Jan 9]. Available from: <https://www.pwc.com/my/en/assets/publications/2021/pwc-deals-strategy-healthcare-in-a-digital-economy.pdf>
63. Lee C, Hutchinson FE. Introduction the Malaysian economy towards 2020 and beyond. Vol. 34, Journal of Southeast Asian Economies. ISEAS - Yusof Ishak Institute; 2017. p. 433–5.
64. Khazanah Research Institute. DIGITAL HEALTH RECORDS IN MALAYSIA THE JOURNEY AND THE WAY FORWARD [Internet]. 2024 May [cited 2025 Jan 9]. Available from: https://www.krinstitute.org/assets/contentMS/img/template/editor/KRI_Digital%20Health%20Records%20in%20Malaysia.pdf
65. Economic Planning Unit. Sixth Malaysia Plan (1991-1995) [Internet]. Prime Minister's Department of Malaysia; 1991 [cited 2025 Jan 9]. Available from: <https://www.ekonomi.gov.my/en/economic-developments/development-plans/rmk/sixth-malaysia-plan-1990-1995>
66. Economic Planning Unit. Seventh Malaysia Plan (1996 - 2000) [Internet]. Prime Minister's Department of Malaysia; 1996 [cited 2025 Jan 8]. Available from: <https://ekonomi.gov.my/en/economic-developments/development-plans/rmk/seventh-malaysia-plan-1996-2000>

67. Malaysia's Telemedicine Blueprint: Leading Healthcare into the Information Age [Internet]. Ministry of Health Malaysia; 1997 [cited 2025 Jan 9]. Available from: <https://www.moh.gov.my/moh/resources/auto%20download%20images/5ca1b20928065.pdf>
68. Ismail NI, Abdullah NH. Developing electronic medical records (EMR) framework for Malaysia's public hospitals. In: 2011 IEEE Colloquium on Humanities, Science and Engineering Research (CHUSER 2011). IEEE; 2011.
69. Economic Planning Unit. Eighth Malaysia Plan (2001-2005) [Internet]. Prime Minister's Department of Malaysia; 2001 [cited 2025 Jan 9]. Available from: <https://ekonomi.gov.my/en/economic-developments/development-plans/rmk/eight-malaysia-plan-2001-2005>
70. Economic Planning Unit. Ninth Malaysia Plan (2006-2010) [Internet]. Prime Minister's Department of Malaysia; 2006 [cited 2025 Jan 9]. Available from: <https://ekonomi.gov.my/en/economic-developments/development-plans/rmk/ninth-malaysia-plan-2006-2010>
71. National Strategic ICT Roadmap [Internet]. Ministry of Science, Technology and Innovation Malaysia; 2008 [cited 2025 Jan 9]. Available from: https://pikom.org.my/wp-content/uploads/2021/04/ICT_Roadmap_Handbook_MOSTI.pdf
72. Economic Planning Unit. Tenth Malaysia Plan (2011-2015) [Internet]. Prime Minister's Department of Malaysia; 2010 [cited 2025 Jan 9]. Available from: <https://www.ekonomi.gov.my/en/economic-developments/development-plans/rmk/tenth-malaysia-plan-10th-mp-2011-2015>
73. Economic Planning Unit. Eleventh Malaysia Plan (2016-2020) [Internet]. Prime Minister's Department of Malaysia; 2015 [cited 2025 Jan 9]. Available from: <https://www.ekonomi.gov.my/en/economic-developments/development-plans/rmk/previous-plans>
74. Health Informatics Centre. Malaysian Health Data Warehouse (MyHDW) 2011-2013. Ministry of Health Malaysia; 2013.
75. Kaos J. Health Ministry Launches Malaysian Health Data Warehouse. The Star [Internet]. 2017 Apr 18 [cited 2025 Jan 9]; Available from: <https://www.thestar.com.my/news/nation/2017/04/18/health-ministry-launches-malaysian-health-data-warehouse/>
76. Kamal SM. Big Data in Healthcare: What We (need to) Know. Malay Mail [Internet]. 2017 Apr 14 [cited 2025 Jan 9]; Available from: <https://www.malaymail.com/news/malaysia/2017/04/21/big-data-in-healthcare-what-we-need-to-know/1360925>

77. Khairie MF, Mazlan N, Mohd Marzuki N, Hussein R. Spatial Analysis of COVID-19: GIS-MyHDW Experience. In: 7th Asia Pacific Conference on Public Health (APCPH) [Internet]. Shah Alam; 2022 [cited 2025 Jan 9]. Available from: <https://apcph.cphm.my/2022/07/spatial-analysis-of-covid-19-gis-myhdw-experience/>
78. Economic Planning Unit. Twelfth Malaysia Plan (2021-2025) [Internet]. Prime Minister's Department of Malaysia; 2021 [cited 2025 Jan 9]. Available from: <https://rmke12.ekonomi.gov.my/en>
79. Pelan Strategik Pendigitalan Kementerian Kesihatan Malaysia 2021-2025 [Internet]. Ministry of Health Malaysia. Ministry of Health Malaysia; 2022 [cited 2025 Jan 9]. Available from: [https://www.moh.gov.my/moh/modules_resources/bookshelf/PELAN_STRATEGIK_PENDIGITALAN_\(PSP\)_KKM_2021-2025/PELAN_STRATEGIK_PENDIGITALAN_\(PSP\)_KKM_2021-2025.pdf](https://www.moh.gov.my/moh/modules_resources/bookshelf/PELAN_STRATEGIK_PENDIGITALAN_(PSP)_KKM_2021-2025/PELAN_STRATEGIK_PENDIGITALAN_(PSP)_KKM_2021-2025.pdf)
80. World Bank. GDP (current US\$) [Internet]. [cited 2025 May 14]. Available from: <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD>
81. World Bank. Population, total [Internet]. 2024 [cited 2025 May 14]. Available from: <https://data.worldbank.org/indicator/SP.POP.TOTL>
82. World Bank. Land area (sq. km) [Internet]. [cited 2025 May 14]. Available from: <https://data.worldbank.org/indicator/AG.LND.TOTL.K2>
83. World Bank. Population density (people per sq. km of land area) [Internet]. [cited 2025 May 14]. Available from: <https://data.worldbank.org/indicator/EN.POP.DNST>
84. World Bank. Current health expenditure (% of GDP) [Internet]. 2025 [cited 2025 May 14]. Available from: <https://data.worldbank.org/indicator/SH.XPD.CHEX.GD.ZS>
85. World Bank. Life expectancy at birth, total (years) [Internet]. 2024 [cited 2025 May 14]. Available from: <https://data.worldbank.org/indicator/SP.DYN.LE00.IN>
86. World Bank. Density of physicians (per 10,000 population). 2024 [cited 2025 May 14]; Available from: <https://data.who.int/indicators/i/CCCEBB2/217795A>
87. Carnicero Giménez de Azcárate Javier, Rojas David. Application of information and communication technologies for health systems in Belgium, Denmark, Spain, the United Kingdom and Sweden. Naciones Unidas, CEPAL; 2010. 89 p.
88. Habicht T, Reinap M, Kasekamp K, Sikkut R, Ewout LA, Ginneken V. Health Systems in Transition Estonia Health system review [Internet]. Vol. 20, W. 2018 [cited 2025 Jan 9]. Available from: <https://iris.who.int/bitstream/handle/10665/330201/HiT-20-1-2018-eng.pdf>

89. Hägglund M, Scandurra I. Patients' Online access to electronic health records: Current status and experiences from the implementation in Sweden. In: Studies in Health Technology and Informatics. IOS Press; 2017. p. 723–7.
90. Doupi P, Renko E, Giest S, Dumortier J. eHealth Strategies Country Brief: Sweden [Internet]. European Commission. 2010 [cited 2025 Jan 9]. Available from: https://ehealth-strategies.eu/database/documents/Sweden_CountryBrief_eHStrategies.pdf
91. Olsson T, Sandström H, Dahlgren P. AN INFORMATION SOCIETY FOR EVERYONE? [Internet]. 2003. Available from: www.sagepublications.com
92. Vision for eHealth 2025 A strategy for implementing [Internet]. Government of Sweden. 2020 [cited 2025 Jan 9]. Available from: https://ehalsa2025.se/wp-content/uploads/2021/02/Strategy-2020-2022_eng.pdf
93. Doupi P, Renko E, Giest S, Dumortier J. eHealth Strategies Country Brief: Denmark [Internet]. European Commission. 2010 [cited 2025 Jan 9]. Available from: https://www.ehealth-strategies.eu/database/documents/Denmark_CountryBrief_eHStrategies.pdf
94. Kierkegaard P. EHealth in Denmark: A case study. J Med Syst. 2013 Dec;37(6).
95. Villumsen S, Faxvaag A, Nøhr C. Development and progression in Danish eHealth policies: Towards evidence-based policy making. In: Studies in Health Technology and Informatics. IOS Press; 2019. p. 1075–9.
96. Making eHealth Work: National Strategy for Digitalisation of the Danish Healthcare Sector 2013-2017 [Internet]. Danish Government. 2013 [cited 2025 Jan 9]. Available from: <https://www.ism.dk/publikationer-sundhed/2013/juni/making-ehealth-work>
97. A Coherent and Trustworthy Health Network For All - Digital Health Strategy 2018-2022 [Internet]. Danish Government. 2018 [cited 2025 Jan 9]. Available from: <https://www.euskadi.eus/dokumentazioa/2020/a-coherent-and-trustworthy-health-network-for-all-digital-health-strategy-2018-2022-healthcare-denmark-2020/web01-a2zesosa/eu/>
98. Price C, Green W, Suhomlinova O. Twenty-five years of national health IT: Exploring strategy, structure, and systems in the English NHS. Journal of the American Medical Informatics Association. 2019 Mar 1;26(3):188–97.
99. Shuttleworth K, Nicholson E. Devolution and the NHS. Institute for Government [Internet]. 2020 Aug 18 [cited 2025 Jan 9]; Available from: <https://www.instituteforgovernment.org.uk/explainer/devolution-and-nhs>

100. Whitehouse D, Giest S, Dumortier J, Artmann J, Heywood J. eHealth Strategies Country Brief: England [Internet]. European Commission. 2010 [cited 2025 Jan 9]. Available from: https://www.ehealth-strategies.eu/database/documents/England_CountryBrief_eHStrategies.pdf
101. Whitehouse D, Giest S, Artmann J. eHealth Strategies Country Brief: Scotland [Internet]. European Commission. 2010 [cited 2025 Jan 9]. Available from: https://www.ehealth-strategies.eu/database/documents/Scotland_CountryBrief_eHStrategies.pdf
102. Whitehouse D, Giest S, Dumortier J, Artmann J. eHealth Strategies Country Brief: Wales [Internet]. European Commission. 2010 [cited 2025 Jan 9]. Available from: https://www.ehealth-strategies.eu/database/documents/Wales_CountryBrief_eHStrategies.pdf
103. Whitehouse D, Walossek U, Artmann J, Giest S. eHealth Strategies Country Brief: Northern Ireland [Internet]. European Commission. 2010 [cited 2025 Jan 9]. Available from: https://www.ehealth-strategies.eu/database/documents/NorthernIreland_CountryBrief_eHStrategies.pdf
104. Kasekamp K, Kalda R. The Milestones of Reforming Primary Health Care in Estonia [Internet]. 2022 Jan [cited 2025 Jan 9]. Available from: <https://www.lshtm.ac.uk/media/59811>
105. Doupi P, Renko E, Giest S, Heywood J, Dumortier J. eHealth Strategies Country Brief: Estonia [Internet]. European Commission. 2010 [cited 2025 Jan 9]. Available from: https://www.ehealth-strategies.eu/database/documents/Estonia_CountryBrief_eHStrategies.pdf
106. Einaste T. Blockchain and healthcare: The Estonian experience. Nortal [Internet]. 2018 Feb 21 [cited 2025 Jan 9]; Available from: <https://nortal.com/insights/blockchain-healthcare-estonia/>
107. Tay C. Electronic Medical Record System to Cost Putrajaya up to RM1.5b. The Edge Malaysia [Internet]. 2019 Jul 3 [cited 2025 Jan 10]; Available from: <https://theedgemalaysia.com/article/electronic-medical-record-system-cost-putrajaya-rm15b>
108. Rasiah R, Rosnah N, Abdullah W, Tumin M. Markets and Healthcare Services in Malaysia: Critical Issues. International Journal of Institutions and Economies [Internet]. 2011 Oct [cited 2025 Jan 10];3(3):467–86. Available from: <https://ijie.um.edu.my/article/view/4831>

109. Farber R, Taylor A. Global Health Diplomacy and Commodified Health Care: Health Tourism in Malaysia and Thailand. *Stud Comp Int Dev*. 2023 Sep 1;58(3):484–510.
110. Sunway Flies High at Healthcare Asia Awards 2024. Healthcare Asia [Internet]. 2024 [cited 2025 Jan 10]; Available from: <https://healthcareasiamagazine.com/co-written-partner/event-news/sunway-flies-high-healthcare-asia-awards-2024>
111. ParkCity Medical Centre bags Healthcare Asia Awards for cutting-edge paediatric ward. Healthcare Asia [Internet]. 2024 [cited 2025 Jan 10]; Available from: <https://healthcareasiamagazine.com/co-written-partner/event-news/parkcity-medical-centre-bags-healthcare-asia-awards-cutting-edge-paediatric-ward>
112. Economic Planning Unit. Malaysia Digital Economy Blueprint [Internet]. Prime Minister's Department of Malaysia; 2021 [cited 2025 Jan 10]. Available from: <https://ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf>
113. Malaysia National Artificial Intelligence Roadmap 2021-2025 [Internet]. Ministry of Science, Technology & Innovation. 2021. Available from: <https://airmap.my/apps>
114. New Milestones for BookDoc in 2020. Malaysiakini [Internet]. 2021 Jan 6 [cited 2025 Jan 10]; Available from: <https://www.malaysiakini.com/advertorial/557725>
115. Jalil A. MHTC partners DoctorOnCall on telehealth services. The Malaysian Reserve [Internet]. 2021 Feb 3 [cited 2025 Jan 10]; Available from: <https://themalaysianreserve.com/2021/02/03/mhtc-partners-doctoroncall-on-telehealth-services/>
116. Baharudin RZ. Futurise - Shaping Malaysia's Regulatory Innovation Landscape. Digital News Asia [Internet]. 2024 Mar 13 [cited 2025 Jan 10]; Available from: <https://www.digitalnewsasia.com/insights/futurise-shaping-malaysias-regulatory-innovation-landscape>
117. Ministry of Science T& I. National Technology and Innovation Sandbox (NTIS) Progress Report 2020-2021 [Internet]. 2021 Aug [cited 2025 Jan 8]. Available from: <https://sandbox.gov.my/report-2020>
118. Md Said F. Empowering Innovation: Strategic Insights into Malaysia's Sandbox Initiatives [Internet]. 2024 [cited 2025 Dec 10]. Available from: <https://techforgoodinstitute.org/blog/expert-opinion/empowering-innovation-strategic-insights-into-malaysias-sandbox-initiatives/>

119. AI Sandbox Launch With NVIDIA [Internet]. Ministry of Science, Technology & Innovation. 2024 [cited 2025 Jan 10]. Available from:
<https://mranti.my/happenings/media-centre/press-release/ai-sandbox-launch-with-nvidia>
120. Government of Malaysia. Medical Act 1971 (Act 50): Incorporating all amendments up to 1 January 2015 [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2015. Available from:
<https://mmc.gov.my/wp-content/uploads/2022/06/Medical-Act-1971.pdf>
121. Government of Malaysia. Nurses Act 1950 (Act 14): Incorporating all amendments up to 1 January 2006 [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2006. Available from:
<https://hq.moh.gov.my/nursing/wp-content/uploads/2015/02/Act-14-06042017.pdf>
122. Government of Malaysia. Medical Assistants (Registration Act 1977 (Act 180): Incorporating all amendments up to 1 January 2002 [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2002. Available from:
https://www.moh.gov.my/index.php/database_stores/attach_download/317/8
123. Government of Malaysia. Allied Health Professions Act 2016 (Act 774) [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2016. Available from:
<https://nutriweb.org.my/pdf/ahp/Allied%20Health%20Professions%20Act%20774%202016.pdf>
124. Government of Malaysia. Private Healthcare Facilities and Services Act 1998 (Act 586): Incorporating latest amendments as of 1 January 2006 [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2006. Available from:
https://www.moh.gov.my/index.php/database_stores/attach_download/317/27
125. Government of Malaysia. Poisons Act 1952 (Act 366): Incorporating all amendments up to 1 January 2006 [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2006. Available from:
<https://pharmacy.moh.gov.my/sites/default/files/document-upload/poisons-act-1952-act-366.pdf>
126. Government of Malaysia. Sale of Drugs Act 1952 (Act 368): Revised 1989, incorporating Act A1084/2000 [Internet]. Commissioner of Law Revision, Malaysia Laws of Malaysia; 2000. Available from:
<https://pharmacy.moh.gov.my/sites/default/files/document-upload/sales-drug-act-1952-act-368.pdf>

127. Government of Malaysia. Medicines (Advertisement and Sale) Act 1956 (Act 290): Revised 1983, incorporating latest amendment – Act A778/1990 [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 1990. Available from: <https://www.moh.gov.my/moh/attachments/1191.pdf>
128. Government of Malaysia. Medical Device Act 2012 (Act 737) [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2012. Available from: https://www.moh.gov.my/index.php/database_stores/attach_download/337/723
129. Government of Malaysia. Private Healthcare Facilities and Services (Private Hospitals and Other Private Healthcare Facilities) Regulations 2006 [Internet]. Commissioner of Law Revision, Malaysia Malaysia: Laws of Malaysia; 2006. Available from: https://www.dataguidance.com/sites/default/files/2_private_healthcare_facilities_and_services_private_hospitals_and_other_private_healthcare_facilities_regulations_2006_002.pdf
130. Kementerian Kesihatan Malaysia. Garis Panduan Pengendalian dan Pengurusan Rekod Perubatan Pesakit di Fasilitas KKM [Internet]. 2021 [cited 2025 Jul 6]. Available from: https://www.moh.gov.my/index.php/database_stores/attach_download/681/206
131. Government of Malaysia. Personal Data Protection Act 2010 (Act 709) [Internet]. Commissioner of Law Revision, Malaysia Malaysia; 2010. Available from: <https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010/>
132. Noor Sureani NB, Awis Qurni ASB, Azman AHB, Othman MB Bin, Zahari HS Bin. The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia. Malaysian Journal of Social Sciences and Humanities (MJSSH). 2021 Oct 10;6(10):488–95.
133. Government of Malaysia. Personal Data Protection (Amendment) Act 2024 (Act A1727) [Internet]. Percetakan Nasional Malaysia Berhad 2024. Available from: <https://www.pdp.gov.my/ppdpv1/akta/pdp-amendmentact-2024/>
134. Hamin Z, Kamaruddin S, Natrah Md Noh H, Bahrin Othman M, Munirah Mohamad A. Recent Reforms to the Personal Data Protection Act 2010 and Its Implications for Business Organisations in Malaysia. Available from: www.rsisinternational.org
135. Government of Malaysia. Communications and Multimedia Act 1998 (Act 588): Incorporating all amendments up to 1 January 2006. Commissioner of Law Revision, Malaysia Malaysia; 2006.
136. Government of Malaysia. Data Sharing Act 2025 (Act 864). Percetakan Nasional Malaysia Berhad Malaysia; 2025.

137. Ministry of Digital Malaysia. Ministry Profile [Internet]. 2024. Available from: <https://www.digital.gov.my/en-GB/profil-kementerian>
138. European Parliament; Council of the European Union; European Commission. Charter of Fundamental Rights of the European Union. Nice, France; 2000.
139. De Hert P, Papakonstantinou V, Malgieri G, Beslay L, Sanchez I. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review*. 2018 Apr 1;34(2):193–203.
140. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [Internet]. Official Journal of the European Union, L168 2024 p. 1–153. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
141. U.S. Department of Health and Human Services. HIPAA Privacy Rule and Its Regulations [Internet]. 2025 [cited 2025 Jul 6]. Available from: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
142. U.S. Department of Health and Human Services. Can health care providers use mobile devices to access or transmit health information? [Internet]. 2015 [cited 2025 Jul 6]. Available from: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html>
143. Rucker DW. Implementing the Cures Act — Bringing Consumer Computing to Health Care. *New England Journal of Medicine*. 2020 May 7;382(19):1777–9.
144. State of California. California Consumer Privacy Act of 2018 (CCPA) [Internet]. California Legislative Information 2018. Available from: https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
145. State of California. California Privacy Rights Act of 2020 (CPRA) [Internet]. California Legislative Information 2020 p. 1–52. Available from: <https://thecpra.org/>
146. U.S. Department of Health and Human Services. 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program [Internet]. 2020 [cited 2025 Jul 6]. Available from: <https://www.govinfo.gov/content/pkg/FR-2020-05-01/pdf/2020-07419.pdf>
147. HL7 International. FHIR® Release 4 (v4.0.1) – HL7 Fast Healthcare Interoperability Resources [Internet]. 2019 [cited 2025 Jul 6]. Available from: <http://hl7.org/fhir/R4/>

148. International Organization for Standardization; International Electrotechnical Commission. ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Geneva, Switzerland; 2019.
149. Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture [Internet]. Gaithersburg, MD; 2020 Aug. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
150. Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations [Internet]. Gaithersburg, MD; 2014 Jan. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf>
151. Khalid M, Kunhibava S. Fintech regulatory sandboxes in Australia and Malaysia: A legal analysis. *IIUM Law Journal*. 2020;28(1):2020–1.
152. Zhi Wei L, Khaw Peng Tsu D. Transforming Mobile Phones into E-Wallets in Malaysia. 2018.
153. Yusoff YH, Jamaludin MN, Ramdan MAA, Abdul Aziz NA, Halim RMM, Abu Bakar MS. Factors Influencing the Emergence of Fintech in Malaysia: A Concept Paper. *International Journal of Academic Research in Economics and Management Sciences*. 2022 Sep 17;11(3).
154. Ministry of Science T and I. National Technology & Innovation Sandbox: 3 Years of Accelerating Evolution of Innovations 2020-2023 [Internet]. [cited 2025 Jan 8]. Available from: <https://sandbox.gov.my/report-2024>
155. Bank Negara Malaysia. Risk Management in Technology (RMiT) [Internet]. 2024 [cited 2025 Jul 7]. Available from: https://bnm.gov.my/documents/20124/938039/ed_RMiT_Nov2024.pdf
156. Open Banking Implementation Entity. Open Banking - A secure way to share your financial data [Internet]. 2024 [cited 2025 Jul 7]. Available from: <https://www.openbanking.org.uk/>
157. Hardt D. The OAuth 2.0 Authorisation Framework (RFC 6749) [Internet]. 2012 [cited 2025 Jul 7]. Available from: <https://datatracker.ietf.org/doc/html/rfc6749>