Navigating Future Management and Ownership of Health Data in 2050, Finland with a Special Focus to the General Data Protection Regulation (GDPR)

Master's thesis
In Future Studies

Author:
Shahriar Ashiqur Rahman

Supervisor:
Juha Kaskinen

31.12.2024
Turku

Master's thesis

Subject: Futures Studies
Author: Shahriar Ashiqur Rahman
Title: Navigating Future Management and Ownership of Health Data in 2050, Finland with a Special Focus to the General Data Protection Regulation (GDPR)
Supervisor: Juha Kaskinen
Number of pages: 59
Date: 31.12.2024

TABLE OF CONTENTS

1. Introduction 6

1.1 Health Data Management and Ownership 7

1.2 Health Data Management and Ownership in the Finland in Current Scenario 8

1.3 Objectives 9

1.4 Research Questions 9

1.5 Structure of the Thesis 9

2 Theoretical Framework 11

2.1 The Definition of Ownership and Property in Legal Context 11

2.2 Special Features of Health Data 12

2.3 Health Data as personal property 13

2.3.1 Right of Alienation 13

2.3.2 Valuation and Compensation 13

2.4 Kremen Requirement 14

2.4.1 Precise definition of health data 15

2.4.2 Capability of Health data for Exclusive Possession of Control 15

2.4.3 Owner's legitimate claim to exclusivity 16

2.4.4 Perennial Duration 17

2.5 Present Legal Position about Health Data in the European Union 17

2.6 Non-proprietary protection of Health Data 19

2.6.1 Medical Secrecy 19

2.6.2 Tort Law 20

2.7 Privacy Challenges 21

2.8 Cyber Security Threats 21

2.9 AI and Healthcare 22

3 Methodology and Research Process 24

3.1 Legal Doctrinal Methodology 24

3.1.1 Application of the Legal Doctrinal Method in Health Data Governance and Identifying relevant Legal Resources 25

3.1.2 The General Data Protection Regulation or GDPR 25

3.1.3 National Laws and Institutions in Finland 29

3.1.4 Case Law Analysis on Data Portability 32

3.2 Multi-Level Perspective 35

- Niche Innovations 36
- Socio-Technical Regime 37
- Assessing Landscape Trends 38

3.3 Scenario Building 40

3.3.1 Patient Centric Ecosystem Scenario 41

3.3.2 Industry-Centric Governance Scenario 43

3.3.3 State-Controlled Data Sovereignty Scenario 45

3.3.4 Fragmented and Inequitable Landscape Scenario 46

3.4 Comparative analysis of the scenarios 48

3.4.1 Comparative Insights 50

3.4.2 Summary Matrix 51

4 Conclusion 53

1. Introduction

The advancement of technology has reshaped the lives of human beings in every sector of our society. In the last few years, our lives have been revolutionized with the inclusion of new medical technological innovations like fitness trackers, smartwatches, different kinds of monitoring devices like continuous glucose monitors, blood pressure monitors, etc., and so on. The expeditious development of technology in the medical arena has resulted in the burgeoning of smart medical devices. Patients' health data can monitor a wide range of physiological variables with these devices, such as sleep patterns, heart rate, and levels of physical activity. These devices constantly collect and transfer huge amounts of health data. This evolution constitutes significant challenges and scopes for the management of health data elevating practical, legal, and ethical questions. Wearable health technology gathers huge volumes of data from its users by using a variety of neurobiological sensors to track both the users' health and their activity levels (Ogundele et al., 2018). Controlling these huge amounts of data can be an uphill problem. Moreover, there is a critical question of who owns valuable health information. Data ownership is a complex and fragmented issue for the present as well as for the future. There are growing concerns on the question of who owns our health data. However, the answer is not simple as there are several stakeholders connected to the issue.

There are also some privacy concerns revolving around these huge health data from different devices. When customers' personal information is gathered in unparalleled quantities, concerns about the user's privacy and safety are raised. (Martínez-Pérez et al., 2015; Ogundele et al., 2018). Health data from smart medical devices can be a reason for concern as it contains various aspects like privacy, security, and ethical considerations. Invasions of privacy may have unintended and potentially damaging repercussions, such as racial profiling, deceptive marketing, and data breaches (Montgomery et al., 2018). There are some legal remedies available to tackle this problem and among them, the most effective one is the European General Data Protection Regulation or GDPR. GDPR contains several rights and duties to enforce data protection rules which are also applicable in the Nordic region. However, it is essential to examine whether legal remedies will be sufficient in the future when more smart medical device users are expected to rise exponentially in the future.

This thesis will delve into complex issues, exploring the future management and ownership of health data by the year 2050 in Finland. It will examine the current legal landscape of data ownership and privacy concerns.

1.1 Health Data Management and Ownership

Health data creates big data. The term "big data" refers to datasets that are so enormous and complex that traditional data processing tools is unable to handle them and analyze them effectively. (Dash et al., 2019). In healthcare, these datasets are derived from multiple sources, including patient medical histories, medical examinations devices etc (Dash et al., 2019). The synthesis and examination of this data can result in substantial enhancements in patient care, operational efficacy, and medical research. It is a huge task to manage this kind of data. Owning health data is also a complex issue. In the current scenario, we have the option only to manage data because of the complexity of health. However, we might to able to own our health data. Medical devices collect a massive amount of data related to our health to improve our lives and provide us with information for the betterment of our health. Therefore we can control and access different approaches to minimize the effect of any disease because of the emergence of huge data (Mirchev et al., 2020). However, the revolution of data creates certain challenges regarding to right to privacy, ownership, control, and management (Mirchev et al., 2020). In the public health system, compulsion exists regarding the use of data to provide better, efficient, and low-priced health care.

On the other hand, data mining is increasing radically in the private health area in the form of selling electronic health records to pharmaceutical companies (Ballantyne, 2020). Health data management is a convoluted matter. Health data, referred to here as HD, collected from individuals, creates a sense of ownership among modern conscious people because we are living in the age of data revolution where data is considered as the ‘the new currency’ or ‘New Oil of the 21st Century’ (Wainwright R, June 8-9, 2011). Not only health companies but also individuals want to utilize their control over health data and this phenomenon is often asserted as the right of ownership of property. It is difficult to determine who owns health data as a plethora of stakeholders are managing data.

The introduction of new technologies and scientific discoveries, as well as the spread of devices that are connected to the Internet, sensors, and mobile applications, are all important contributors to the rise in the number of intelligent devices that can be integrated into human beings. Today, smart medical devices are rapidly gaining popularity, expanding, and gathering momentum for usage in both personal and professional settings.

The majority of smart medical devices, such as bands, watches, blood pressure monitors, and so on, are designed to be more compact and easily connected to one's body. This contrasts with the size of electronic devices such as smartphones and tablets. More privacy concerns are brought about by medical devices to the individuals who are wearing them and who are surrounded by them as a result of their widespread adoption by both the consumer and enterprise sectors.

1.2 Health Data Management and Ownership in the Finland in Current Scenario

The management and ownership of health data in Finland are governed by rigorous legal frameworks, such as the General Data Protection Regulation (GDPR), and national laws such as the Data Protection Act and the Act on the Secondary Use of Health and Social Data. These legal frameworks are adopted to ensure that health data is being managed and owned appropriately. Patients' rights, data security, and transparency are given the highest priority under this legislation. Through the utilization of technologies such as Kanta Services, patients are able to gain access to and exercise control over their own health data. These technologies also contribute to the availability of interoperability for medical practitioners. The management of large amounts of data in the healthcare industry presents a number of challenges, such as issues with the privacy of customers' data, the requirement for extensive processing resources, and the difficulty of integrating different types of data (Dash et al., 2019).

The current state of health technology in the Nordic countries is characterized by an environment that encourages innovation and large-scale investment. This region has a significant amount of untapped potential in health technology. The Nordic countries have established themselves as leaders in health technology as a consequence of their inventive

mind-set, world-class healthcare systems, and robust infrastructure. When it comes to the law, however, ownership is still unclear, and the focus is more on data control than it is on ownership itself. Individual privacy is protected while also improving medical research and public health thanks to Finland's forward-thinking regulations.

1.3 Objectives

This paper will attempt to analyze health data ownership in the current and future legal regime. This thesis will also look into ethical considerations posed by the data ownership issue.

The thesis will seek to enter the conversation on the future implications of the right to privacy. This thesis will also examine future scenarios for 2050 to provide a comprehensive understanding of future ownership of health data in Finland.

1.4 Research Questions

i. What are the ethical implications of health data ownership in Finland by 2050, and how are these considerations influencing legal frameworks?
ii. How will the evolving technological landscape and regulatory frameworks in Finland shape the future ownership of health data by 2050?

1.5 Structure of the Thesis

- **Introduction**

The first chapter will cover the introduction portion of the ownership of data and the right to privacy, as well as the aims and research topics that will be addressed.

- **Theoretical Framework**

The second chapter will conduct an analysis of theoretical components, which will cover topics such as ethical considerations about ownership of health data, AI in healthcare and privacy issues in an assortment of legal circumstances.

- **Methodology and Research Process**

The third chapter will look over the methodology and research procedure. In addition to legal doctrinal methodology, a multilevel perspective will be utilized in this thesis to achieve its objectives.

- **Conclusion**

The concluding chapter will comprise a discussion of the findings accompanied by recommendations.

2 Theoretical Framework

Patient data ownership has become a debatable issue with the emergence of data driven world and the inclusion of artificial intelligence in the present era. There are both positive and negative arguments for owning health data by the patients. Moreover, several frameworks and solutions have been given regarding the management of health data. There is a lot of complexity surrounding the idea of ownership of individual health data, and it is possible that it does not adequately address the ethical and practical difficulties of data access and exchange. (Piasecki & Cheah, 2022). There should be a more nuanced approach to navigate these challenges. In this chapter, I will examine the theoretical point of view of ownership of patient data from an ethical legal and perspective.

2.1 The Definition of Ownership and Property in Legal Context

To ascertain the ownership of data, firstly, it is essential to ascertain if health data qualifies as personal property. The issue of patient information proprietorship necessitates the justification of "self-ownership" which is considered a modern term of, *property of his own person*, by John Locke in 1680 (John, 2018; Macpherson, 1962; Tully, 1993). According to John Locke, "*every man has a property in his own person: thus, nobody has any right to but himself"*. The characteristics of personal health data cannot be differentiated from the individuals. Westin suggested the notion that private data ought to be officially acknowledged as a unit of ownership rights (Pateman, 2002; Westin & Freedom, 1967). To assess the relevance of property rules to health data, it is essential to analyze the characteristics of health data within the framework of property law.

The state of absolute rights and property is known as ownership from a legal context (Liddell et al., 2021). An association between an individual and a thing is often considered as property. On the other hand, property rights bring about obligations and responsibilities between individuals to protect the correlation that exists between a person and a thing. Therefore, Property is commonly described as a 'bundle' or 'collection.' (Liddell et al., 2021). There are mainly two sticks in this bundle. One is the right to exclude, and another is alienability. The core argument for a right to exclude is related to the property owner's jurisdiction and ascendency over the property (Liddell et al., 2021). This right should not be mixed up with the right to us of the property. One example of someone who has the

exclusive right to use a piece of property is the person who owns that piece of land. The owner's ability to grow livestock or build a vehicle repair shop may be constrained by land use regulations. (Liddell et al., 2021).

2.2 Special Features of Health Data

The issue of whether the law should acknowledge patients as proprietors of certain health data is complicated by the diverse characteristics of such data.

Firstly, health information can have both medical and confidential affectability (Liddell et al., 2021). A person's weight and height describe a patient. From the point of view of a medical doctor, these seemingly negligible facts can occasionally be helpful in the diagnosis of risk factors or health disorders such as different kinds of diabetes and heart disease. Patient's height and weight data can be a basic characteristic of numerous health care. The consultants might use it as their private data. However, the patients also treat it as personal and private. If somehow the data is disclosed, it would create problems for both healthcare providers and patients resulting in economic loss or embarrassment. **Secondly**, the significance of health data alters broadly depending on how and by whom the information is collected. Both the doctor and the patient could find some data completely useless, while other data could be very important for healthcare. **Thirdly**, health data may include personal information about third parties. **In the fourth place**, the patient is not the only person who is involved in the generation of health information; rather, there are typically a large number of parties and devices participating (Ballantyne, 2020). A primary diagnostic would not reveal the real disease. For example, a patient going to the doctor for hemorrhoid treatment could be subjected to fatty liver disease after a blood test or another examination. In this setting, health information encompasses a wide range of data, such as the patient's description of injury, the patient's own self-described symptoms, and the data obtained from the investigation of that presenting complaint. To put it another way, health information is produced and generated through a series of intricate procedures that involve the use of bodies, awareness, interpretation, measurement, labor, expertise, judgment, and various pieces of technology. In order to develop health information, it is vital to have both the patient and the professional involved, but this alone is not adequate.

2.3 Health Data as personal property

There is little discussion about when health data would be properties under a traditional framework for personal property. In this section, we will try to see structural issues if health data is regarded as personal property.

2.3.1 Right of Alienation

The right of alienation has long been seen to be one of the most significant rights associated with property. As a result, the courts have made substantial efforts to avoid any voluntary constraints on the capacity of an owner to transfer ownership of their property because of this perception (Contreras, 2019).

Academics have proposed revised interpretations of the right to alienate to mitigate the impact of unrestricted alienability by subsequent holders of personal data. These concepts originate from the inherent divisibility of property rights. Diverse concurrent utilizations and interests in actual and intellectual property exemplify the diversity of property rights seen in both categories of property. Thus, akin to a book or musical work safeguarded by intellectual property rights, personal data may be licensed just for certain purposes authorized by the owner.

2.3.2 Valuation and Compensation

The right to be paid to the property is closely associated with the right to alienate. Charging for the use of health data is regarded as one of the main reasons to propertize HD. With the help of health data discoveries or new research have been carried out. Some discoveries create huge amounts of money and sometimes the data is used for only educational or research purposes. Therefore, it is difficult to charge for health data in every circumstance. There are also other problems.

Firstly, it is nearly impossible to value health data because sometimes those can be part of a profoundly big research or medicine discovery. So, there is no way to measure the contribution of the individually provided data.

Secondly pharmaceutical or biotech companies are sometimes unwilling to pay royalties to the developers who create inventive tools for them (Murray, 2010). Consequently, it will be impracticable to think that those companies are going to pay the HD owners for their little to no contribution (Terry et al., 2007).

Thirdly, if we characterize health data as a commodity, then it would hamper the research for new drugs or vaccines. As solvent people would not want to commercialize their privacy to companies for monetary value, health data from different sections of society would be difficult to retrieve effecting the efficaciousness and authenticity of the health data research (Posner, 1978, pp. 397 - 398).

Finally. If an individual wants to control their health data, he/she has to avail of advanced technological means to control HD.

2.4 Kremen Requirement

Various propositions have been put up to legalize HD by granting all of the property rights that are governed by common law (Contreras, 2019, p. 635). In order to give this strategy more power, a brand-new system of property rights needs to be constructed from the ground up. The legislative method is more favorable than the judicial approach because, in an ideal world, legislative procedures include more refining and customization (Contreras, 2019). The Ninth Circuit Court in the USA applied a three-part test on whether intangibles can be considered property in Kremen vs Cohen("Kremen vs Cohen," 2003). This case provides a detailed analytical framework on what characteristics the intangibles should have to be considered as property (Contreras, 2019, p. 635). The three-part framework for assessing property like nature on an intangible are:

i) the need for a precise definition;
ii) the capability of exclusive possession or control;
iii) establishing a legitimate claim to exclusivity (Contreras, 2019, p. 636).

2.4.1 Precise definition of health data

It is difficult to ascertain the precise definition of health data because of its huge amount of data and the uncertainty of the health conditions of an individual. For example, a person could catch a cold before expressing symptoms of it. The question is when the information can become your property before or after the symptoms are visible. Or if one has a fever but does not own a thermometer, he or she buys it after one day. In this case, the question is when the temperature becomes its own property. Generally, one does not need to be consciously aware of the property existing like you might own a piece of land under which there are gold bars without your knowledge (Contreras, 2019, p. 637).

So according to common property law, you would be the owner. With this logic, both known and unknown health data can be considered as property. However, if the patient's condition changes every hour, then the data could be measured in which way like every second or every hour. Therefore, it is difficult to find a 'precise definition' under the *Kremen* standard.

2.4.2 Capability of Health data for Exclusive Possession of Control

The exclusivity of health data poses another challenge to consider it as property. HD cannot be claimed as a sole proprietary right as there are many stakeholders involved in different medical procedures like MRI, CT scan, ECG blood pressure monitoring, etc. Even if one has access to this data, there is a question of whether these data can be stored. Physical property can be locked or other intangibles like monetary interests can be kept with electronic security with the help of banks. However, in the case of health-related data, a healthcare facility has the sole control to store and manage it. The patients cannot have exclusive possession of the data. Even if someone authorizes any third party like a healthcare facility to manage the data. If a doctor measures a patient's pulse or blood pressure, the person might be prohibited from disclosing the data at that point by law, but the question is whether it can be prevented in the future. Therefore, possession of exclusive control over health data is nearly impossible to achieve.

2.4.3 Owner's legitimate claim to exclusivity

The third factor is whether property owners have legitimate claims over property. In the *Board of Regents of State Colleges v. Roth, the court* stated that “To have a property interest, it is evident that a person needs more than just a want or a need for something to have that interest. It is impossible for him to merely expect it to happen. Rather than that, he needs to be able to demonstrate that he is qualified to receive it.” When a person owns or buys a property, that person spends money, time, and labor to make the property his own. However, in the case of HD, the individual contributed profoundly little or no effort at all to achieve it (Contreras, 2019). Health data from patients mostly contains descriptive information. The person invests a small quantity of energy, time, or resources into creating information.

Experts with specialized knowledge like doctors, pathologists, medical examiners, etc.) generally find and analyze this data. Moreover, they evaluate it independently of the patient. The sole thing that the individual has is the expectation of having complete control over the situation. In point of fact, the individual only possesses an "abstract need or desire" to get ownership of their health data. Even if a rational patient had the ability to possess exclusive control over health data, he or she would be sensible enough not to attempt to enforce exclusivity against a physician who had gotten independent health information from her. There are a number of factors that can limit the legitimacy of an individual's assertion of exclusive rights over health data. These factors include social welfare considerations in addition to individual self-interest. There will be some problems if patients have a legitimate claim of exclusiveness of health data. Firstly, it would hamper the scope of bio medical research which is very important in the health and medical industry. Secondly, medical professionals will lose the ability to interact with public health authorities and they will be unable to report significant health-related observations, such as outbreaks of infectious diseases, novel strains of influenza, symptoms that were not previously known, and adverse drug responses. Moreover, the authorities in charge of public health will be precluded from making use of the data and acting on the information.

2.4.4 Perennial Duration

In general, ownership of property remains property to the person who has legal authority over it. It can never become obsolete. As health data is stout in nature and hard to relinquish, recognizing it as a property would create some limitations to make it permanent property (Contreras, 2019). **Firstly**, a particular data may be useful for a research organization for a long time. For example, medical data for the coronavirus would not be relevant even not be used forever. Because of the fact that studies cross-index and build upon one another, it is highly implausible that scientists or medical professionals will also engage the same data in the future. (Contreras, 2019, p. 648). It is astonishing how difficult it is to keep track of this data through continuous generations of studies that do not make use of primary data but instead depend on the consequences and conclusions of earlier studies. (Contreras, 2019). **Secondly**, the level of complexity continues to rise when it comes to investigations that involve epidemiological and population observations. For example, widespread HIV-affected patients research would not only include the affected people but also uninfluenced people who are in control groups. A large portion of the population is ensnared in a plethora of such studies (Contreras, 2019). It is possible that the intricacy involved in such an endeavor would be insurmountable. This is because traditional property interests do not vanish even as they become compact pieces of comprehensive data.

2.5 Present Legal Position about Health Data in the European Union

A legal system can establish a framework of property rights by determining ownership and delineating the conditions under which such rights may be infringed upon. Courts from different legal systems have considered whether intangible assets like HD can be recognized as property over the years. In general, courts have considered intangibles like shares in a corporation ("Payne v. Elliot," 1880), data in a customer sheet, Domain names on the Internet ("Kremen vs Cohen," 2003), franchised businesses("Hatfield v. Straus," 1907), or degrees of medical profession("O'Brien v. O'Brien," 1985) , etc. as property. Some intangibles that courts do not deem properties are hot news("Int'l News Serv. v. Associated Press," 1918), the authority to have law enforcement enforce a restraining

order ("Town of Castle Rock v. Gonzales," 2005), the government's right to regulate arms sales ("United States v. Evans," 1988), and citizens' rights ("McNally v. United States," 1987) , etc.

Generally, health data is not considered as property in the current legal arena. However, there are some laws which play an essential role to ensure secure management of health data.

- **General Data Protection Regulation (GDPR)**

A key framework for the management of health data within the European Union (EU), the General Data Protection Regulation (GDPR) places an emphasis on the protection of personal data while simultaneously encouraging innovation and the exchange of data across international borders. Given the sensitive nature of health data, which is a particular category under the General Data Protection Regulation (Article 9), it is necessary to implement additional protections. By pseudonymizing and anonymizing data, GDPR encourages innovation and makes it possible for secondary applications of health data in research while maintaining privacy (Hoerbst & Ammenwerth, 2010).

- **European Health Data Space (EHDS)**

The groundbreaking European Union initiative known as the European Health Data Space (EHDS) aims to create a unified system for the administration of health records. Primary and secondary uses of health data will be made easier across all member states by this approach. The objective of the 2022 plan known as EHDS is to facilitate the exchange of health data across national boundaries in a way that is secure, standardized, and interoperable. Following the guidelines laid out by the GDPR, this is done in a lawful manner. To further facilitate safe data sharing and ensure compliance, EHDS also establishes a health data access body in every member state. According to Hoerbst and Ammenwerth (2010), the European Health Data System (EHDS) promotes cooperation and new ideas in order to make the EU a leader in regulating health data in a way that is ethical, compatible, and focused on patients. The exploitation of EHDS health data is driven by the core goal of enhancing healthcare services for individuals. When countries use standardized EHR systems, people's medical records can be easily accessed and shared across borders. The two main advantages of this interoperability are the increased patient agency over their own data and the enhanced continuity of therapy. The secondary

use of health data that has been anonymized or pseudonymized by EHDS is made possible by secure access and can assist research, innovation, policymaking, and public health. Keeping users' privacy preserved, the initiative encourages the safe and voluntary sharing of health data for the benefit of society, with a focus on data altruism.

- **European Directive 96/9/EC**

Under European Directive 96/9/EC, health data might be regarded as property. It is a special protection under the directive. From the point of view of the regulation, the term "database" refers to any type of information that is organized in an orderly or systematic fashion and may be accessed on an individual basis through electronic transmission or some other means.

- **Cross-Border Healthcare Directive**

The Cross-Border Healthcare Directive, also known as Directive 2011/24/EU, makes it easier for people of the European Union to obtain healthcare services that are both safe and of high quality in all member states. A directive that was adopted in 2011 assures that patients can seek treatment in other countries within the EU and be paid for their expenses under certain circumstances. To ensure that patients receive consistent care, it encourages collaboration between national healthcare systems and places an emphasis on the interoperability of electronic health records (EHRs) and electronic prescriptions.

2.6 Non-proprietary protection of Health Data

It is clear that health data is not considered property because of its unique nature. Health data has some characteristics of being property. However, are few key indicators of property are missing from health data. This does not mean the health data cannot be protected. There are some non-proprietary rights to provide remedies in case of violation of health data rights. Those are discussed below:

2.6.1 Medical Secrecy

Generally, health data always comes under medical secrecy. Whether it is a public or private healthcare provider, they have a responsibility to protect the confidence of their patients (Liddell et al., 2021). They should not exploit or disclose data without the permission of their customers. Nonetheless, the duty is not obvious. There is a possibility that it will be rendered obsolete by other elements that influence the efficiency of modern

healthcare systems. Courts have pursuit these reflections consciously stabilizing public and private interests. Informed consent is profoundly important for revealing patient data. The patients must be completely notified of how their information is used and shared. Providers sometimes must share health data because of responding to subpoenas, or notifications from public health authorities. In the United Kingdom, the NHS Act 2006 specifies this duty of confidentiality under section 251. Medical secrecy does not only safeguard personal privacy but also encourages trustworthiness between healthcare and patients. This will promote open and honest communication. Technological innovations like electronic health records have developed the management and sharing of health data. However, there are some impediments to maintaining confidentiality. Data intrusion and cyber assaults on healthcare systems demonstrate the relevance of vigorous cybersecurity measures to protect critical health data. Disclosure might be needed in order to analyze reports on finances and data on technology systems for auditors and computer professionals. In the European Union, the General Data Protection Regulation or GDPR.

2.6.2 Tort Law

The law of tort provides a comprehensive legal remedy for addressing the misuse of health data. The law of tort also enables individuals to claim compensation for damage caused by health data infringement. Concerns regarding invasions of privacy and unauthorized uses of patient data are raised when a healthcare provider divulges health information without first obtaining the patient's appropriate permission. The law of tort enables various infringements in case of mishandling of health data. In general, the violation types include negligence, breach of confidentiality, invasion of privacy, defamation, strict liability, etc. The claim of negligence can be used against health care providers who are unable to exercise the customary steps to protect health data. Misuse of health data could result in strict liability. Strict liability is a conception applied in both civil and criminal law that holds a party liable for their actions regardless of their intention at the time of the action. Some jurisdictions enforce strict liability on providers handling sensitive health data. They can be held liable for misuse regardless of fault or negligence. Moreover, a patient can pursue a defamation claim if false information is provided by the health care facility. Therefore, the patient’s reputation is at stake.

2.7 Privacy Challenges

It is the responsibility of the customers to provide their personal data. Personal data can be protected by setting up passwords in open devices and applying further passwords as security measures to safeguard private information in apps (Sainz-de-Abajo et al., 2020). Data pertaining to health is extremely sensitive and important, making it an essential area of concentration for the preservation of privacy in the digital age. The proliferation of electronic health records (EHRs), wearable devices, and analytics driven by artificial intelligence presents substantial privacy challenges in relation to the acquisition of data, the sharing of data, and the protection of data. Different app stores have various kinds of apps, where scammers try to set traps to violate personal data. Likewise, health application data can also be violated by scammers. Therefore, a verification process can be introduced in app stores to detect malware in applications (Sainz-de-Abajo et al., 2020). Patients, doctors, family members, and scientific investigators may have access to confidential data that is acquired by mobile health applications. However, it is also possible that this information might be shared with other parties, such as marketers, which raises serious concerns regarding the confidentiality of the information that is obtained from consumers (Sainz-de-Abajo et al., 2020). Health professionals are using more Electronic Health registers and electronic health care. Health service providers are facing immense security and privacy challenges in keeping the integrity, confidentiality, and availability of customer information (Wang et al., 2013). Various sources have been producing enormous volumes of heterogeneous data. The health industry sector has been presented with the necessity to manage this data (Kumar et al., 2018).

2.8 Cyber Security Threats

Among the many difficulties associated with health data management, cybersecurity concerns rank high. The public's faith in health data management systems can be eroded, services can be disrupted, and sensitive patient information can be compromised as healthcare systems digitize their operations. In order to improve patient care and operational efficiency, healthcare organizations have embraced electronic health records (EHRs), wearable devices, and analytics powered by artificial intelligence (AI). Malicious actors now have a larger target to exploit because of this digital revolution. Healthcare systems are frequently the targets of phishing, ransomware, and Distributed

Denial of Service (DDoS) assaults. Data leaks, unauthorized access to sensitive health information, and system shutdowns are all possible outcomes of cyberattacks. To illustrate the point, consider the 2017 WannaCry ransomware attack in the UK, which disrupted the National Health Service (NHS), delayed treatment, and exposed holes in the healthcare industry's cybersecurity architecture. (Khan et al., 2023).

Information pertaining to a person's health, including their medical records, genetic makeup, and lifestyle choices, is among the most delicate forms of personal data. The hefty black-market value of stolen health records makes them an attractive target for cybercriminals. The documents can then be utilized for blackmail, insurance fraud, or identity theft (Bhuyan et al., 2020). Unlike financial data, which can be reset (e.g., credit card numbers), health data breaches have long-term consequences as medical records cannot be changed. Due to limited resources, antiquated systems, or inadequate employee education, many healthcare businesses do not have strong cybersecurity frameworks. Healthcare systems that are more than a decade old are frequently vulnerable to cyberattacks because they cannot keep up with the latest security standards (Martin et al., 2017).

Cloud computing, Internet of Things devices, and artificial intelligence (AI) all work together to make healthcare more vulnerable. A malicious actor might trick an AI system into prescribing the wrong medication or making an incorrect diagnosis. (Reddy et al., 2020). When data is stored on the cloud, it creates a dependent on third-party providers, which raises issues about illegal access and inadequate security standards.

2.9 AI and Healthcare

The amalgamation of artificial intelligence (AI) in healthcare has revolutionized the management and analysis of health data, offering opportunities for personalized medicine, predictive analytics, and improved patient outcomes. However, the use of AI raises critical questions about the ownership of health data, particularly as data generation, processing, and sharing increasingly involve private entities and automated systems.

For artificial intelligence systems to be able to train their algorithms and provide reliable insights, they require vast datasets. Electronic health records (EHRs), diagnostic tools, and wearable devices often contain sensitive personal information that is included in these datasets. Because numerous parties, such as patients, healthcare providers, and technology businesses, contribute to and use these datasets, the use of health data in artificial intelligence raises questions regarding data governance and ownership.

When data from patients is used to develop insights provided by artificial intelligence, such as diagnostic forecasts or individualized treatment plans, the ownership of health data becomes especially unclear. AI systems generate new outputs that add value, and these outputs could be claimed by developers or healthcare providers. Patients are the source of the raw data. Concerning who controls these outputs and who gains from their commercialization, this creates problems that are both ethical and legal in nature.

Profit is frequently prioritized over patient rights in the process of commercializing AI-driven health solutions, which might result in the potential exploitation of sensitive data. It is also possible that unequal access to artificial intelligence technologies can make existing healthcare disparities even worse. It is essential to have open and honest agreements on the use of data and ownership in order to safeguard patient rights while simultaneously encouraging innovation.

3 Methodology and Research Process

This thesis combines the Legal Doctrinal Method with the Multi-Level Perspective (MLP) to examine the ownership and management of health data in Finland by 2050. The future of health data governance is shaped by the interconnections of evolving technologies, regulatory frameworks, and societal trends.

MLP provides a socio-technical perspective to examine these interactions. The current legal landscape, including data protection regulations in Finland and the General Data Protection Regulation (GDPR), can be systematically examined using the Legal Doctrinal Method. By bringing these approaches together, we can examine health data ownership and management from a sociotechnical and legal perspective. In this chapter, I will discuss the legal doctrinal methodology and multilevel perspective in the context of health data management in Finland.

3.1 Legal Doctrinal Methodology

The word ‘doctrine’ originated from the Latin word ‘doctrina’. It means to teach, to instruct. Doctrinal research concentrates on examining and elucidating legal documents, such as statutes, case law, and regulations, in understanding legal perspectives, principles, and doctrines. The emergence of the Roman Legal Doctrine started before the birth of Christ and achieved profound importance in the third century (Van Hoecke, 2011). During the Middle Ages legal doctrine was regarded as a scientific discipline, however, after the mid-nineteenth century it was concluded that the basic characteristics of becoming a ‘legal science’ were missing from legal doctrine (Van Hoecke, 2011). Before that legal doctrine was widely observed to be model science. There are some criticisms against legal doctrinal methodology. It is too illustrative and autopoietic. The method of legal doctrine is very similar to those legal practices and it is myopic because of specialization and geographical limits (Van Hoecke, 2011). When it comes to publications, there is not much of a distinction between those written by legal practitioners and those written by legal scholars. The Legal Doctrinal Method is a rudimentary approach to legal research. It is often regarded as a ‘black letter law’ approach. The method entails a systematic investigation of legal doctrines, cases, legislation, and other authoritative sources to elucidate and evaluate the legal principles and contexts associated with a particular issue (Hutchinson, 2013).

3.1.1 Application of the Legal Doctrinal Method in Health Data Governance and Identifying relevant Legal Resources

The Legal Doctrinal Method provides the foundation for analyzing the existing legal landscape and identifying areas for reform in response to future challenges. The process involves systematic analysis of statutory laws, case law, and academic interpretations. This method is particularly significant for evaluating health data because it enables a comprehensive study of existing legal frameworks, the discovery of deficiencies, and the investigation of how existing laws may evolve in response to future technological developments. Consequently, this approach is useful for evaluating health data management in real-life situations.

3.1.2 The General Data Protection Regulation or GDPR

According to article 5, the General Data Protection Regulation provides several principles such as purpose limitation, data minimization, lawfulness, transparency, confidentiality, and accountability.

- **Purpose Limitation and digital minimization:** Health data must be collected for specific and limited purposes. If the purpose is fulfilled the data should not be used in other matters. Moreover, the data should be used based on necessity.
- **Lawfulness and transparency:** Health data should be used according to the lawful manners mentioned in article 6 of the GDPR or in the case of public welfare and scientific research.
- **Integrity and confidentiality:** Pseudonymization and encryption are two instances of the proper technical and organizational measures that ought to be enforced by organizations that deal with health information in order to guarantee its safety.

3.1.2.1 Ownership of Health Data under GDPR

GDPR does not specifically vest in ownership rights to individuals over their health data. However, the regulation provides data subjects rights which gives remarkable

control over their health data, effectively giving them quasi-ownership. The rights which can be connected to health data rights are given below:

- **Right of Access by the Data Subject:** Patients or individuals have the right to access their health data. The article empowers the owner of the data subject to review how it is being used and stored. The individual should have the right to be informed when personal health data are transferred to a third country or an international organization.
- **Right to Data Portability:** An individual has the right to receive his or her health data in a structured machine-readable format. Moreover, the right to transfer the data to different service providers has also been given in accordance with GDPR.
- **Right to be Forgotten:** Data can be requested to be deleted or erased by fulfilling specific conditions. This right ensures a high level of control of user's health data.
- **Right to Restriction of Processing:** An individual's right to restrict access to their health data is contingent upon the circumstances. The conditions include unlawful data processing, questions on the accuracy of the health data, or veracity of the data based on legal grounds (Article 18, GDPR).

3.1.2.2 Health Data and GDPR in Practice

The incorporation of the GDPR in the management of health data entails substantial ramifications for healthcare providers, researchers, and technological businesses. Healthcare services need to figure out a balance between the obligation to follow GDPR and the requirement to use health data for improving patient care and enabling medical innovation.

- **Explicit Consent**: Researchers face challenges while collecting explicit consent, and using health data in processing activities. These activities are profoundly important for clinical trials. Therefore, they need to negotiate stringent consent requirements. AT the same time, it is necessary to comply with the exemption of the GDPR in Public Health and scientific research.
- **Pseudonymization and Anonymization**: The GDPR promotes pseudonymization or anonymization as a method for processing health data more

flexibly while maintaining individual privacy. Pseudonymized data is still classified as personal data, although anonymized data is exempt from the GDPR, allowing for its broader application in research (Mantelero & Review, 2018)

- **Cross-Border Data Sharing**: The GDPR imposes rigorous requirements on the transfer of health data outside of the European Union. Organizations should make certain that adequate protection is in place before transmitting data over international borders. These safeguards may include typical contractual requirements or adequacy decisions.

3.1.2.3 Definition of 'Data Controller' and 'Data Processors'

It is important to define data controllers and data processors as they have lots of powers and responsibilities that can affect the rights of individuals.

- **Definition of Data Controller**

GDPR defines "data controller" in article 4(7). Any organization, individual, or government body that determines the purpose and means of processing personal data is known as a data controller. The controller is ultimately responsible for making sure that data processing follows the guidelines of the GDPR. These principles encompass ideas such as legality, equity, openness, reduction of data, and purpose restriction. (Article 5, GDPR).

- **Data Controller's Responsibilities**

The data controller's responsibilities include;

The controller must establish a legal basis to ensure the individual's right to consent. The lawful basis is also required for other purposes like public interest or medical purposes.

Controllers should also maintain transparency. They must provide clearly expressed data subjects so the receivers can understand how their data is collected, analyzed, and used (Article 12, GDPR).

Through the management of Data Protection Impact Assessments (DPIAs) for the purpose of high-level risk processing and the maintenance of records of processing operations, they shall demonstrate compliance with the General Data Protection Regulation (GDPR). Article 32 empowers controllers to implement appropriate technical and organization measures to protect data. The measures include encrypting or pseudonymizing data.

- **Definition of Data Processor**

According to GDPR, the organization that processes personal data on behalf of the controller is referred to as a data processor. The data controller is the one who gives the instructions to the processors, and the processors are not the ones who decide the aims or the ways of processing.

- **Data Processor's Responsibilities**

Data processing is key to analyzing data to use it for different purposes According to GDPR data processor cannot process data on its own. According to article 28 of GDPR, the processor can only process after getting documented instructions from the controller. In the event that a processor decides to work with another processor, known as a sub-processor, they are required to obtain prior written authorization from the controller and ensure regulation through contractual agreements.

Article 33 states that the processor has also the responsibility to implement security measures to protect personal data. If there is any breach of data protection, the processor must inform the controller. (Article 32)

- **Relationship between Data Controller and Processor**

The GDPR stipulates a clearly defined relationship between the data controller and the data processor to ensure responsibility, transpicuousness, and compliance in personal data handling. The structure of this relationship is designed to clearly define duties and responsibilities, hence reducing the amount of ambiguity that exists over the processing and protection of data. GDPR places an emphasis on the contractual relationship that exists between controllers and processors. It mandates the creation of a legally enforceable agreement that explains the terms. However, the controller holds absolute responsibility, and the role of a processor is to maintain compliance. Both organizations may be subject to penalties for non-compliance, which highlights the importance of working together and establishing robust contractual agreements in order to successfully secure personal data.

3.1.2.4 Challenges Of Health Data and Compliance of GDPR

It is clear that there is no specific expression that states health data ownership in GDPR. Health data is considered as sensitive data according to article 9 and this ambiguity poses significant implications. GDPR empowers an individual to exercise

different rights such as data portability or eraser, however, they do not own the health data in a traditional way. There is still no clear definitive concept of ownership, which makes concerns regarding accountability and data-sharing agreements more complicated. There is an area of legal uncertainty that arises when trying to determine who the proprietor of health data from smart medical devices or electronic health data becomes. Businesses that use health data for artificial intelligence-driven analytics or tailored medicine may assert that they have the right to process such data in order to protect their legitimate interests, which can lead to conflicts between individual rights and economic interests (Tikkinen-Piri et al., 2018). GDPR also does not address the growing commercialization of the health data.

Within the realm of large-scale data sharing and analytics, the severe consent procedures and data localization laws imposed by the GDPR may impede medical research and innovation. On the user's part, sometimes they were unaware of the extent of data processing, reducing their effective control. Fitness wearables or smart medical devices depend on a model of implied consent or bundled agreement.

3.1.3 National Laws and Institutions in Finland

Finland has enacted several laws and regulations to implement and adapt GDPR in its national laws. The scope of different laws expands to the secondary use of data, electronic systems, and patients' rights. The following part will discuss Finnish national laws and institutions, which play a key role in managing health data.

3.1.3.1 Data Protection Act (1050/2018)

The Finnish Data Protection Act integrates the provision of GDPR for the purpose of processing data in the public sector and defining the roles of supervisory authorities. The act provides a description of the duties of the health care service providers as data controllers. Moreover, the act plays a focal role in ensuring the usage of health data in a lawful, transparent, and secure way. Significantly, the legislation places an emphasis on the limitation of objectives and the minimization of data, with the goal of ensuring that health information is only used for authorized and specified purposes.

3.1.3.2 Secondary Use of Health and Social Data (552/2019)

The act on the Secondary Use of Health and Social Data can be considered one of the most innovative legal remedies for managing the growing significance of health data. The objective of the law is to manage the use of health data beyond primary healthcare activities. There are various aspects included such as research, science, or policy making. This law opens the door to the establishment of Findata. It is a centralized authority responsible for giving permits for the secondary use of health and social data. Findata takes measures to ensure that data is anonymized or pseudonymized, and that secondary use is following ethical and legal norms when applicable.

Before any personal information can be processed, individuals are required to give their informed consent, as stipulated by the GDPR. This provision, however, is subject to several exceptions that are outlined in the Secondary Use Act. These exceptions include situations in which processing is required for research or when it serves the public interest.

Ethical oversight is also mentioned in this law. The processing of health data must conform to strict ethical practices in order to guarantee that individual rights are upheld. Moreover, the act also ensures that social benefits are generated at the same time (Tikkinen-Piri et al., 2018).

3.1.3.3 Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007)

Finland has introduced a digital platform, for storing and sharing electronic health records, known as Kanta Services. This is also officially known as the Kanta Services Act or the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare. Kanta services not only allow patient to access their prescriptions, treatment history, and medical history but also empower healthcare providers to share information securely. Patients are given the autonomy to review and control their own health data that is stored in Kanta. This involves the ability to restrict access to particular data they have stored. According to the act, healthcare providers are required to utilize systems that are compatible with Kanta and integrate with it. This ensures the sharing of data in a seamless manner while preserving privacy and security.

3.1.3.4 Patient Act (785/1992)

Confidentiality and the right to access medical records are key fundamentals of the Act on the Status and Rights of Patients. By allowing individuals to control how their data is accessed and shared, as well as by mandating that healthcare providers protect patient data, the Patient Act strengthens the principles underlying the GDPR.

3.1.3.5 Institutional Roles in Health Data Management

Several institutions play a profound role in the implementation of the Finnish health data laws.

- **The Office of the Data Protection Ombudsman**

Protecting people's privacy and rights is a top priority for Finland's Office of the Data Protection Ombudsman, especially because digitalization is revolutionizing the management of personal and health data. Maintaining trust in Finland's data-driven healthcare system is facilitated by the Ombudsman's efforts to ensure GDPR compliance and solve new difficulties.

The Office instructs enterprises and the general public on how to comply with the General GDPR and manage personal data in a manner that is both ethical and legal. It does this by issuing recommendations and providing interpretations of complicated data protection legislation in order to simplify requirements, particularly in sensitive industries such as academia and healthcare.

The ombudsman is required to collaborate with other EU data protection authorities. It is a member of the European Data Protection Board (EDPB), which coordinates the implementation of the GDPR across the European Union. Individuals can lodge complaints with the ombudsman if they believe their data protection rights have been infringed because of different anomalies like failure to honor data access or erasure requests or if their consent is not taken in accordance with the GDPR requirements.

- **Kanta Services**

Kanta Services is a digitalized health information platform which is operated by the Social Institution of Finland also known as Kela. Kanta Services is responsible for ensuring the safe storage, access, and interoperability of electronic health records (EHRs)

and other health-related information throughout the whole healthcare system in Finland. This service strengthens Finland's commitment to efficient and transparent health data management. Kanta Service securely keeps medical records, medications, and treatment information from both private and public healthcare. This service managed electronic health records, e Prescriptions and medical histories, laboratory and diagnostic data.

By guaranteeing the secure transmission of data between healthcare practitioners across institutions, Kanta improves the efficacy of care coordination. Interoperability standards decrease therapy-related errors and increase treatment efficiency by making sure authorized providers have access to updated patient information. By guaranteeing the secure transmission of data between healthcare practitioners across institutions, Kanta improves the efficacy of care coordination. Interoperability standards decrease therapy-related errors and increase treatment efficiency by making sure authorized providers have access to up-to-date patient information. Kanta service also integrates the Secondary Use of Health and Social Data Act in various areas like research and policy making. To ensure that secondary use is in accordance with ethical and legal criteria, the platform implements procedures such as pseudonymization and data anonymization.

- **Findata**

The primary role of Findata is to facilitate the safe and ethical secondary use of health and social data for different purposes like statistics, research, and policy-making. Findata is established under the Act on the Secondary Use of Health and Social Data. Organizations or researchers who want access to health data should apply to Findata. Findata reviews applications for legal and ethical standards and it grants access to aggregated and pseudonymized data to protect individual identities. Findata also integrates data from different sources like electronics health records from Kanata Service, national health and social care registries, and other relevant public and private sources.

3.1.4 Case Law Analysis on Data Portability

Case law analysis is profoundly important to analyze the application of statutes and regulations in practical cases. Moreover, it reflects how courts deal with complex and abstruse situations regarding a particular circumstance.

3.1.4.1 Schrems v. Facebook Ireland

An individual has the right to get the data in a machine-readable format. The importance of the right to data portability can be seen in **Schrems v. Facebook Ireland**[1] Facebook Ireland Ltd. and Max Schrems, an Austrian privacy campaigner, were involved in a historic lawsuit that brought attention to the idea of data portability in accordance with the GDPR. In accordance with Article 20 of the GDPR, Schrems exercised his right to data portability. This provision enables individuals to request that their personal data be presented in a format that is structured, frequently used, and machine-readable. This gives them the freedom to move their data to another service provider. Schrems requested not only all his personal data from Facebook but also inferred or derived data created by Facebook, such as profiling information and analytics ("Schrems v. Facebook Ireland," 2018). The argument put up by Schrems is that the definition of personal data under the GDPR encompasses both raw data and inferred data, with the latter being obtained directly from the activities and interactions of the user. He also complained about Facebook's failure to fulfils its obligation to provide his data in a required format. Specifically, the case brought up problems regarding the limitations of data portability, specifically whether it applies just to data that is "provided by the data subject" or whether it extends to data that is generated through processing operations ("Schrems v. Facebook Ireland," 2018). The Austrian Data Protection Authority came to the conclusion that Facebook was not required to include any data that was inferred or derived in its response to the data portability inquiries. Article 20 of the General Data Protection Regulation (GDPR) makes a clear reference to data that is "provided by the data subject," which means that it does not include data that is created by the controller through analysis or profiling.

3.1.4.2 Danish Consumer Council vs Telecom Company

A notable case, Danish Consumer Council vs Telecom Company, on the importance of data portability, **concerns** the failure of a telecommunications firm to deliver client information in a portable format, the Danish Consumer Council has filed a complaint. The rights of individuals to access and transfer their personal data, as well as the obligations of data controllers, are discussed in this case, which provides insights into

[1] Case C-498/16.

both concepts. As previously discussed, data portability enables individuals to switch service providers by receiving data in a structured machine-readable format and transferring data to another controller.

In response to many customers' requests for their personal information made to a telecom operator under Article 20 of the General Data Protection Regulation (GDPR), the Danish Consumer Council has launched a complaint on their behalf. Data portability requirements of the General Data Protection Regulation (GDPR) were not met by the company. Instead, it sent the information in a proprietary format that couldn't communicate with other telecom companies' networks. In response to many customers' requests for their personal information made to a telecom operator under Article 20 of the GDPR, the Danish Consumer Council has launched a complaint on their behalf. The company did not meet the data portability requirements of the GDPR. Instead, it sent the information in a proprietary format that couldn't communicate with other telecom companies' networks.

The plaintiffs argued that their right to data portability was infringed as the data requested, was not in a machine-readable format and they could not be transferred to other telecom operators. The significance of data portability in the advancement of consumer rights and regulations was reaffirmed by this verdict. Competition. The defendant argued that the failure of the other operators to understand the data led to that situation after they already transferred the data.

The court ruled in favor of the Danish Customer Council. The court stated that GDPR requires the data to be provided in a commonly used and machine-readable format. Due to its incompatibility with other service providers' proprietary formats, the telecom company's format fell short of this requirement. It is necessary for organizations to make certain that their systems are capable of extracting data in portable formats, which necessitates adaptations to both the technological and procedural aspects.

3.1.4.3 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)

This case is significant for the Right to be forgotten but also addressed principles relevant to data portability. In the year 2014, Mario Costeja González informed the Spanish Data Protection Agency (AEPD) of his intention to lodge a complaint. Seeking the erasure of personal information linked to his name in Google's search results. The complaint was made against Google Spain and Google Inc. Despite the fact that the case was primarily concerned with the Right to Erasure, it nevertheless made a passing reference to the problem of data portability by posing questions concerning the obligations of data controllers in the management of personal data. This case clarified search engines' position as data controllers, and they are responsible for complying with data subject requests like data portability. The data controllers are also responsible for providing accessible data and transferring or removing the data upon request ("Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.," 2014). This issue was requested by the plaintiff, Mario Costeja González. The court ruled under EU law Google can be considered a controller, and it is responsible for data processing and securing compliance with user requests. This case also laid the foundation for ensuring the right to data portability by reinforcing user empowerment in managing personal information.

3.2 Multi-Level Perspective

One of the most popular socio-technical approaches, known as the Multi-Level Perspective (MLP), is utilized to get an understanding of how transitions in technology and society take place on three different levels: the niche, the regime, and the landscape (Geels & transitions, 2011). Niches are safeguarded environments where groundbreaking discoveries, whether novel technologies or experimental policies are cultivated. These inventions frequently confront established systems yet necessitate cultivation to endure. Niches are essential for promoting creativity and experimentation, as they serve as a proving ground for concepts that may transform broader systems.

The regime signifies the prevailing structures, conventions, and behaviors within a specific system. This includes rules, institutions, technologies, and cultural norms that reinforce existing systems.

The regime offers stability and predictability; nonetheless, it is marked by path dependency, rendering it resistant to disruptive advances. The landscape includes extensive societal, economic, and environmental developments that affect both the regime and niches. These trends represent external forces, whether demographic shifts, political movements, or global crises, that exert pressure for systemic change.

To examine health data governance in Finland, MLP is particularly well-suited since it enables an investigation into how developing technology, current healthcare systems, and broader societal trends interact to influence future legal and regulatory requirements.

- **Niche Innovations**

At this tier, you can find the most avant-garde and revolutionary ideas, practices, and technology that arise from the margins of society. Emerging technologies, like wearable medical devices or AI-driven health diagnostics, encounter initial resistance but, with support, might pose a threat to established systems. Actors create, test, and improve innovative ideas in niches.

For mapping niche-level innovations, the first step is to identify emerging technologies that generate health data.

The advent of AI has been a game-changer in the healthcare industry, opening up new possibilities in areas such as customized medicine, diagnostic accuracy, and predictive analytics. Machine learning algorithms sift through mountains of medical records in search of trends, which pave the way for earlier diagnosis and more personalized treatment plans (Topol, 2019). Artificial intelligence combined systems raise some essential questions on data ownership, consent, and transparency.

For sharing data between health care providers and third-party applications growing interoperability solutions like Fast Healthcare Interoperability (FHIR) APIs, contribute a pivotal role in the current world of technological advancement. The innovative technologies decrease data silos and enhance the process of portability (Mandel et al., 2016)

Wearable devices like fitness watches and trackers, smartwatches, and smart medical devices generator gigantic amounts of consecutive health data. These smart devices

enable an individual to monitor their health and these data also create new challenges regarding data portability and privacy. Distributed ledgers that cannot be altered are made possible by blockchain technology, which enables the secure management of medical records. Blockchain technology helps to alleviate issues regarding trust and security in multi-stakeholder systems by enabling the sharing of data that is both transparent and unchangeable. The usage of blockchain technology in applications such as MedRec allows for the maintenance of electronic health records, which guarantees the integrity of the data and gives patients control over the permissions they have to access their records.(Azaria et al., 2016)

- **Socio-Technical Regime**

The regime comprises established structures, norms, and practices that govern a system, including healthcare policies, professional practices, and current health data legislation in Finland. Regimes exhibit stability and resistance to change as a result of path dependency and entrenched interests. Nonetheless, they are sometimes compelled by specialized developments or external influences. Finland's healthcare institutions have demonstrated adaptability in responding to the dual pressures of technological advancements and evolving regulatory frameworks, such as the GDPR**.** By leveraging centralized health systems like Kanta Services**,** integrating advanced technologies, and aligning with national and EU policies, Finland ensures its healthcare system remains innovative and compliant. Kanta Service helps Finland's healthcare institutions by providing a centralized platform for electronic health records (EHRs) and patient access to health data. Kanta's unique interoperability feature enables healthcare providers to share patient information and enhance their treatment efficaciousness. Institutions have been encouraged to increase Kanta's security measures, including data encryption and access restriction, as a result of regulatory demands like the GDPR emphasis on data openness and patient rights. These initiatives comply with the GDPR requirements for securing accountability and privacy.

Tools such as artificial intelligence (AI), telemedicine, and wearable gadgets have been adopted by Finland's healthcare institutions in order to handle the demands that have been brought about by the rapid advancement of emerging technologies. AI-driven solutions, such as diagnostic algorithms and predictive analytics, improve decision-making but can present compliance difficulties. These solutions are examples of AI-driven solutions. Data Protection Impact Assessments or DPIAs are carried out by institutions according

to the GDPR for high-risk processing activities. This helps to ensure that artificial intelligence is deployed in a lawful and ethical manner (Topol, 2019). Moreover, a wearable device is significantly integrated with patient care. This new trend opens the path for the new regime of data governance to address privacy and portability concerns. Finland's national legislation such as the Act on the Secondary Use of Health and Social Data should comply with GDPR. Under the careful supervision of both ethical and legal standards, this legislation makes it possible for institutions to reuse health data for innovation and research. In Finland, the data permit authority known as Findata plays a crucial part in the management of secondary data use. Its primary responsibility is to ensure that institutions comply with openness and privacy rules while simultaneously encouraging innovation (Testa, 2022). Collaborating with technology providers, legislators, research groups, and healthcare institutions work together to manage the challenges that come from both technical advancements and regulatory mandates. Through these relationships, it is possible to co-create solutions that are in compliance with the law while also meeting the requirements of the healthcare industry. Tackling the pressure of technological advances and regulatory innovations, Finland has adopted centralized systems and new technologies with the integration of GDPR and other national laws. Finland has emerged as a global leader in digital health governance by balancing innovation with patient treatment.

MLP asserts that transitions arise when niche innovations get momentum and correspond with landscape-level forces, resulting in a reconfiguration of the regime. The incorporation of AI in healthcare and the emergence of digital privacy movements have compelled governments to conform to GDPR and evolving health data management protocols (Geels & Schot, 2007).

- **Assessing Landscape Trends**

The landscape level includes extensive cultural, economic, and political patterns that impose enduring pressures on both niches and regimes. Examples encompass demographic shifts, escalating privacy apprehensions, or international efforts such as the General Data Protection Regulation (GDPR). Landscapes frequently serve as external influences that define the setting for transformations. Finland's health data management system is going through an evolutionary process. The health data management sector in Finland is influenced and shaped by societal trends, economic trends, and global adaptations. This discussion will examine how these macro-level forces influence niche innovations like artificial

intelligence or wearable technologies and their relationship with the sociotechnical regime of establishing health systems. By the year 2050, the interaction between these forces will have a substantial impact on the governance of Finland's health data, necessitating the implementation of flexible policies and technology. In the following, I will assess different, specifically three types of trends such as *societal*, economic, and global, which are relevant to the landscape level.

Societal Trends include growing public awareness of privacy. Public awareness of Privacy protection is largely dependent on the management of health data in Finland. Niche regimes are being prioritized to uphold transparency and consent because of public concerns about data protection. These concerns are influenced by alarming data breaches and the global situation. It will continue to be of utmost importance to comply with the GDPR, which necessitates the creation of patient-centered solutions that create a balance between innovation and ethical data use. Chronic Diseases and Aging Populations: It is a significant societal factor that Finland's population is getting older. In Finland, by the year 2050, approximately thirty percent of the population will be over the age of sixty-five, which will lead to an increase in the number of chronic diseases such as diabetes and cardiovascular problems (Finland, 2015). This development requires niche innovations like wearable devices or telemedicine platforms to enable real-time monitoring. At the same time, interoperable systems like Kanta Services should be integrated by healthcare providers.

Because of the increasing commercialization of health data, the economic landscape of Finland is undergoing a complete transformation. Research in the fields of pharmaceuticals, insurance modeling, and artificial intelligence (AI) all consider health data to be a valuable resource. The sociotechnical regime is responsible for a number of obligations, including the regulation of commercialization in order to safeguard against exploitation and the promotion of public-private partnerships that bring together economic benefits and social welfare (Mantelero & Review, 2018). The healthcare system in Finland is facing increasing pressure to maintain cost control while also providing high-quality care. Because of this economic need, the use of predictive analytics based on artificial intelligence is being driven in order to maximize resource allocation and eliminate hospital admissions. Artificial intelligence (AI) and blockchain are examples of specialized technologies that offer cost-effective solutions for the secure sharing of data. On the other hand, the sociotechnical regime is responsible for ensuring

that these innovations are incorporated into the appropriate regulatory and operational frameworks, with a particular focus on affordability and equity.

Because of the rapid growth of AI technology, health data governance is facing consequences. There are several ethical concerns in AI-driven healthcare. The concerns include biases in transparency and algorithms. These are affecting niche innovations and regimes. The institutions of Finland are required to establish methods such as Algorithmic Impact Assessments (AIAs) and include worldwide norms on the ethics of artificial intelligence in order to align themselves with international best practices (Topol, 2019). As a result of globalization, there is a greater demand for the exchange of data across international borders in order to progress medical research and tackle global health emergencies such as pandemics. The European Health Data Space or EHDS is one of the initiatives that intends to establish a single framework for the sharing of data among the countries that make up the European Union. In order for Finland to be successful, it will be essential to align specialty developments with EHDS needs. In order to improve interoperability and guarantee compliance with international standards, the sociotechnical regime needs to be made more effective. The socio-technical regime and specialized innovations are both affected by societal, economic, and worldwide developments, which are changing the face of health data administration in Finland. The need for strong regulatory frameworks is driven by the adoption of cutting-edge technologies, which are in turn driven by demographic shifts, economic challenges, and international programs like EHDS. Finland's health data ecosystem, which aims to balance innovation, ethical governance, and society's well-being, will be defined by its capacity to harmonize these forces.

3.3 Scenario Building

The Multi-Level Perspective (MLP) framework provides a systematic perspective to analyze the future of health data management in Finland. The niche, sociotechnical regime, and landscape level trends are profoundly significant to examining different trends and scenario building of health data management in the year 2050 in Finland. These levels are also important for exploring the four alternative scenarios namely: Patient-Centric Ecosystem, Industry-Centric Commercialization of Health Data, Government-Led Centralized Data Sovereignty, and Fragmented and Inequitable Health Data Landscape.

3.3.1 Patient-Centric Ecosystem Scenario

In this scenario, Finland establishes a robust legal framework that explicitly recognizes patients as the primary owners of their health data. Empowered by GDPR and national laws, patients control how their data is accessed, shared, and monetized. This scenario builds on robust regulatory frameworks, including enhanced provisions under the GDPR, to establish explicit ownership rights for individuals over their health data. By leveraging cutting-edge technologies and fostering ethical practices, this ecosystem ensures that patients are at the center of data-driven healthcare systems.

3.3.1.2 Key Characteristics of the Scenario

- **Explicit Ownership Rights**

Patients are the principal owners of their electronic health records, wearables, and insights generated by AI. This includes the raw data from these sources. To ensure that individuals are able to restrict access, dictate usage conditions, and monetize their data if they so choose, legal revisions in Finnish law have clearly defined these rights.

- **Transparent and Ethical Data Governance**

Patients have the ability to provide or remove access to their data in real-time, which is made possible by digital tools, which help to strengthen consent systems. While at the same time respecting the privacy of individuals, ethical rules make certain that health data is utilized for the benefit of society, such as in the area of public health research.

- **Data Management**

Patients can share their data in a secure manner with healthcare practitioners, researchers, or private organizations through the use of smart contracts, which automate data-sharing agreements. The technology known as blockchain makes it possible to store and manage data in a decentralized way, which guarantees trust, transparency, and transparency.

- **Interoperability**

Compliance with the European Health Data Space guarantees that Finnish systems are integrated with frameworks that are used across the EU, which in turn encourages collaboration between healthcare providers from different countries. Because data systems are fully interoperable, it is possible to share patient information without any

interruptions across national borders, between research institutes, and between healthcare practitioners.

3.3.1.3 Driving Factors

- Finnish laws align with EU initiatives like the EHDS, ensuring a harmonized approach to data governance. GDPR's principles are expanded to include explicit ownership rights, strengthening individual control, and enhancing privacy protections.
- Blockchain, AI, and wearable technologies become widespread, enabling secure, transparent, and efficient data management. Machine learning algorithms personalize healthcare services, improving patient outcomes.
- Rising public awareness of data privacy and security drives demand for patient empowerment in health data governance. A cultural shift toward individual autonomy reinforces the importance of ethical and transparent data practices.

3.3.1.4 Outcome

- **Equity and Access**

All patients, irrespective of socio-economic position, gain advantages from interoperable systems and equitable healthcare services. Regional differences in access to modern technology are mitigated.

- **Trust and Transparency**

A trusting relationship between patients, healthcare providers, and other stakeholders can be fostered through the implementation of transparent data-sharing procedures and robust privacy measures.

- **Innovation and Economic Growth**

The deployment of data-sharing methods that are open and transparent, as well as effective privacy controls, can help to create a relationship of trust between patients, healthcare professionals, and other stakeholders alike.

3.3.1.4 Challenges

It is necessary to make substantial investments in both infrastructure and human resources in order to successfully implement decentralized systems with contemporary technologies. The instruction of digital literacy would be challenging to accomplish. Because of this, it would be difficult to ensure that all individuals are able to traverse digital tools and understand their rights, which would require significant efforts to be made in the field of public education.

3.3.2 Industry-Centric Governance Scenario

In the **Industry-Centric Governance** scenario, private corporations dominate the health data ecosystem in Finland by 2050. This model prioritizes rapid innovation and economic efficiency, driven by significant investments in advanced technologies for example artificial intelligence (AI), wearable devices, and data analytics. However, the emphasis on profitability leads to ethical concerns, reduced equity, and challenges in maintaining public trust.

3.3.2.1 Key Features of the Scenario

- **Corporate Dominance**

  There is a fragmented environment that has been created because of the replacement of public management systems like Kanta Services with proprietary platforms. Companies are the ones that establish the standards for data governance. The majority of health data systems, such as electronic health records (EHRs), diagnostic tools based on artificial intelligence, and wearable ecosystems, are managed by multinational corporations and private enterprises individually.

- **Profit-Driven Innovation**

  A wide variety of commercial uses, including pharmaceutical research, insurance modeling, and the development of healthcare products, make substantial use of health data. Artificial intelligence-driven analytics, precision medicine, and personalized healthcare technologies are all experiencing tremendous developments as a result of corporate investments.

- **Limited Interoperability**

For the purpose of safeguarding their competitive edge, businesses uphold proprietary data standards, which ultimately leads to the creation of siloed systems with restricted data portability.

- **Healthcare Inequities**

  Advanced healthcare services are accessible to those who can afford premium offerings, creating disparities in access and outcomes. Public healthcare systems lag behind, relying on outdated technologies due to limited funding and a reliance on private-sector solutions.

3.3.2.2 Key Driving Forces

- As the expense of healthcare continues to rise, governments are being forced to outsource the maintenance of health data and the development of new technologies to private corporations. The treatment of health data as a valuable economic resource is what drives the involvement of corporations and the commercialization of health data.
- The integration of Finland's health data ecosystem with global data markets has resulted in the country becoming a hub for foreign businesses, but it has also resulted in a reduction of national control over sensitive health data.

3.3.2.3 Outcome

Finland's economy receives a considerable boost from the commercialization of health data, which in turn brings in investments from other countries and generates employment opportunities in the health technology sector. Individuals with higher incomes have a disproportionate share of the benefits that premium services and cutting-edge technologies provide, whereas economically disadvantaged people have restricted access to high-quality medical care. As a result of the widening of regional imbalances, rural areas and public systems are falling more and further behind urban centres and private services. Patients are becoming increasingly sceptical of the motivations of corporations, particularly in regard to the ethical usage of data and the privacy protection.

3.3.2.4 Challenges

- The government's ability to defend patient rights and implement GDPR principles is diminished as a result of inadequate oversight, which allows firms to dominate data governance.
- Public opposition to injustices and a lack of transparency may grow, which would impede further innovation and the uptake of corporate-led solutions.

3.3.3 State-Controlled Data Sovereignty Scenario

Under the State-Controlled Data Sovereignty model, the Finnish government views health data governance as a public good and assumes complete ownership and control over it. By restricting the influence of the corporate sector, this centralized strategy promotes equity, public accountability, and data sovereignty. Ethical and safe data management is ensured through the strengthening of regulatory frameworks to correspond with GDPR principles and national objectives. There is a constant stream of new innovations, but scalability and agility are hindered by inefficient governmental procedures and a lack of private sector involvement.

3.3.3.1 Key Characteristics of the Scenario

- **Centralized Data Management**
  Finland's government consolidates all health data under a single, state-controlled platform. An expanded **Kanta Services** serves as the backbone of this centralized system. The platform integrates data from (EHRs), wearables, and AI-generated analysis, ensuring a unified and secure infrastructure.

- **Universal Access and Equity**
  The government ensures equitable access to healthcare services powered by data, reducing disparities between urban and rural populations. All citizens, regardless of socio-economic status, benefit from state-controlled technological advancements.

- **Data Sovereignty and Security**
  Finland asserts full sovereignty over its health data, reducing reliance on multinational corporations for storage or processing. Strict cybersecurity measures

and GDPR-compliant practices are implemented to protect sensitive data and prevent breaches.

3.3.3.2 Key Driving Forces

- The public's faith in government-run services is on the rise due to rising worries about corporate abuse of data and privacy. Instead of valuing quick technological advancement, citizens place a premium on openness and equal access.
- Finland aligns with global movements emphasizing data sovereignty to protect national interests and citizen rights. Collaboration within the **European Health Data Space (EHDS)** ensures compliance with EU regulations while preserving national control.

3.3.3.3 Outcome

The distribution of healthcare services is fair, guaranteeing that no population is disadvantaged. Care in Finland is of a consistent high standard, reducing inequalities by region. Public sector priorities, rather than market competition, promote innovation at a modest pace. The implementation of innovative technology may be hindered due to the lack of collaboration with private entities. Citizens have faith in the ethical and secure use of personal data when their government is open and honest with them about how it plans to use it. Data is only utilized for objectives that are in line with public welfare, thanks to government control.

3.3.3.4 Challenges

Potentially lowering Finland's competitiveness in the global health tech industry, limited private-sector involvement could impede technological developments. Delays in implementing new technology and decision-making could result from centralized governance.

3.3.4 Fragmented and Inequitable Landscape Scenario

In the Fragmented and Inequitable Landscape scenario, Finland's health data governance in 2050 is marked by disconnected systems, inadequate regulatory supervision, and pronounced discrepancies in healthcare access and quality. Discrepant policies, inconsistent technological uptake, and conflicting stakeholder interests result in

inefficiencies, distrust, and stagnation in the management and ownership of health data. This situation illustrates the dangers of not synchronizing technological, legal, and societal progress under a unified framework.

3.3.4.1 Key Characteristics of the Scenario

- **Technological Silos**

Public and private healthcare providers implement incompatible data systems, resulting in data silos that obstruct interoperability and data portability. Efforts to synchronize systems under the European Health Data Space (EHDS) framework are unfinished, hindering cross-border cooperation and data exchange.

- **Uneven Access to Innovation**

Wealthy regions and private institutions have access to advanced technologies like AI-driven diagnostics and wearable health devices. Public healthcare systems and rural areas lag behind, using outdated technologies and providing limited services.

- **Lack of Public Trust**

Frequent data breaches, opaque data-sharing practices, and unethical commercialization lead to widespread public distrust in both public and private healthcare systems. Patients hesitate to share their health data, further limiting innovation and collaboration.

3.3.4.2 Driving Factors

- There is a lack of coordination between the GDPR, Finnish regulations, and real life practices in the commercial sector, which results in inconsistencies in data governance. Both gaps in healthcare access and data infrastructure are made worse by the limited public funding and uneven regional development that exists.
- Despite the fact that they operate without enough oversight or ethical requirements, private firms dominate certain elements of health data management.

3.3.4.3 Outcome

- The lack of clarity around ownership rights and the frequent exploitation of patients' data causes patients to lose confidence in healthcare-based systems. Individuals are

reluctant to disclose their health data for the purposes of study or innovation, which is detrimental to public health initiatives.

- Advanced healthcare services are only available to wealthy populations, while economically disadvantaged people are confronted with fewer options and lower outcomes. Regional imbalances continue to widen, with metropolitan centers reaping the benefits of investments made by the private sector while rural areas continue to lag behind.

3.3.4.4 Challenges

Without clear legal frameworks, disputes over data ownership and commercialization rights become more frequent, further delaying progress. Unchecked commercialization and data misuse by private companies exacerbate public mistrust and raise ethical questions. Fragmentation limits the ability to leverage Finland's health data for large-scale studies and international collaborations.

3.4 Comparative analysis of the scenarios

Each of the four scenarios—the Fragmented and Inequitable Landscape, the State-Controlled Data Sovereignty, the Industry-Centric Governance, and the Empowered Patient Ecosystem—presents a unique perspective on the future of health data governance in Finland. The contrasts between them across important variables are shown in the table below.

Dimension	**Empowered Patient Ecosystem**	**Industry-Centric Governance**	**State-Controlled Data Sovereignty**	**Fragmented and Inequitable Landscape**
Governance	Decentralized, patient-driven;	Centralized, controlled by	Centralized, government-	Disjointed, weak regulatory

	legal frameworks empower individual ownership.	private corporations; profit driven.	led with strong regulatory control.	oversight, competing interests.
Ownership	Patients have explicit ownership and full control over their data.	Ownership remains ambiguous; corporations control derived data.	Ownership is public, with the government acting as the custodian.	Unclear ownership; frequent disputes over data control.
Innovation	High and inclusive; patient participation drives advancements.	Rapid but profit-focused; innovation benefits affluent groups.	Moderate; driven by public-sector priorities, slower than private-led models.	Stagnant due to lack of coordination and trust.
Equity	High; all citizens benefit from transparent systems and ethical commercialization.	Low; significant disparities based on economic and regional factors.	High; universal access is ensured by state control.	Low; rural areas and public systems lag behind private advancements.
Trust	Strong; transparency and ethical practices foster patient trust.	Moderate; scepticism over corporate motives and data privacy.	Strong; citizens trust government oversight and public welfare focus.	Weak; data misuse, breaches, and lack of transparency erode trust.
Interoperability	High; seamless cross-border and	Limited; proprietary systems create	High; centralized platforms	Low; incompatible systems hinder

	system-level data sharing.	silos and restrict portability.	ensure interoperability within public systems.	data sharing and collaboration.
Economic Model	Ethical commercialization: patients receive fair compensation for data use.	Profit-driven commercialization with limited patient benefits.	Publicly funded; minimal private-sector involvement.	Inefficient resource use; overlapping systems increase costs.
Global Influence	Finland leads as a model for ethical and patient-centric health data governance.	Finland excels in innovation but loses ethical leadership.	Finland champions equitable governance but is less competitive globally.	Finland loses relevance in global health data collaboration.

3.4.1 Comparative Insights

- **Governance Models**

Patient-Centric Ecosystem: Decentralized systems empower individuals but require robust legal and technological infrastructure. **Industry-Centric Governance**: Centralized under private corporations, this model sacrifices equity and trust for rapid innovation. **State-Controlled Data Sovereignty**: Centralized government control ensures equity but faces challenges with scalability and innovation speed. **Fragmented Landscape**: Weak coordination leads to inefficiencies, mistrust, and stagnation.

- **Data Ownership**

Explicit patient ownership is a cornerstone of the **Empowered Patient Ecosystem**, whereas **Industry-Centric Governance** leaves ownership ambiguous, favoring corporations. **State-Controlled Data Sovereignty** treats data as a public good, ensuring

equitable use but limiting individual autonomy. **Fragmented Landscape** offers no clear ownership structure, causing disputes and inefficiencies.

- **Equity and Access**

Empowered Patient Ecosystem and **State-Controlled Data Sovereignty** provide equitable access, reducing disparities. **Industry-Centric Governance** and **Fragmented Landscape** exacerbate inequalities, favouring wealthier populations or regions.

- **Innovation and Progress**

Innovation thrives in **Industry-Centric Governance** due to corporate investments but comes at the cost of equity. The **Empowered Patient Ecosystem** balances inclusivity with innovation, leveraging patient participation. **State-Controlled Data Sovereignty** achieves steady but slower progress. **Fragmented Landscape** struggles with innovation due to disjointed systems and public mistrust.

- **Trust and Transparency**

Strong trust is a hallmark of the **Empowered Patient Ecosystem** and **State-Controlled Data Sovereignty**, driven by transparency and ethical governance. **Industry-Centric Governance** has moderate trust due to concerns about corporate motives, while trust is weakest in the **Fragmented Landscape** scenario.

3.4.2 Summary Matrix

Dimension	**Best Scenario**	**Worst Scenario**
Governance	Patient-Centric Ecosystem	Fragmented and Inequitable Landscape
Ownership	Patient-Centric Ecosystem	Fragmented and Inequitable Landscape
Innovation	Industry-Centric Governance	Fragmented and Inequitable Landscape
Equity	State-Controlled Data Sovereignty	Industry-Centric Governance

Trust	Patient-Centric Ecosystem	Fragmented and Inequitable Landscape
Global Leadership	Patient-Centric Ecosystem	Fragmented and Inequitable Landscape

The comparative analysis highlights the **Empowered Patient Ecosystem** as the most balanced and sustainable future for health data governance in Finland. It combines innovation, equity, and trust by centering patient rights and ethical practices. Conversely, the **Fragmented and Inequitable Landscape** represents a cautionary tale, emphasizing the need for cohesive strategies and collaboration among stakeholders. Strategic investments in technology, legal reforms, and public trust-building will be essential to navigate toward a desirable future.

4 Conclusion

Health data ownership is both a multidimensional and complicated topic because of the sheer amount of data processing happening in a very short period of time. By analyzing health data management and ownership in Finland, several recommendations can be proposed to tackle the emerging challenges. To strengthen the robustness of health data management and foster innovation, the proposals will play a pivotal role in tackling challenges in a rapidly growing socio-technical environment.

Firstly, there should be a clear provision regarding health data ownership in Finish legislation to ascertain ownership rights in health data. Both GDPR and Finnish laws emphasize data subject rights such as portability, erasure, or access. However, the regulations do not specify ownership in different circumstances like multi-stakeholder environments involving patients, healthcare companies, and private entities. Therefore, legal clarity will enable a person to exercise his rights in an efficacious manner and controllers or processors can operate within well-defined boundaries.

Secondly, Finland ought to work toward enhancing its technological standards to improve interoperability and portability. Among these is the implementation of open, machine-readable formats that are compatible with systems all around the European Union, as envisioned by the European Health Data Space Project. Even though the General Data Protection Regulation (GDPR) advocates strongly data portability, there are still problems that prevent smooth data sharing between platforms. Because it enables seamless transitions between healthcare providers and allows for the incorporation of future technologies such as wearables, interoperability is a crucial component in the process of realizing the full potential of digital health systems. There should be greater emphasis placed on Findata's role in the supervision of technical compliance and standardization. Kanta Services is one example of a national health system that has included many emerging technologies to ensure the secure sharing of data.

Thirdly, there ought to be ethical rules and revenue-sharing arrangements for the commercialization of health data. To cultivate trust and equity, patients whose data contribute to artificial intelligence training or commercial applications ought to be compensated fairly or provided with related benefits. While the commercialization of

health data, which is driven by private enterprises and improvements in artificial intelligence, presents a tremendous opportunity for innovation, it also poses a risk of patient data being exploited. In order to strike a balance between ethical values and commercial objectives, a framework is required. It is recommended that a public-private collaboration be established in order to cultivate business interests and guarantee the transparency of data monetization.

Fourthly, the government ought to initiate nationwide campaigns with the purpose of enhancing digital health literacy and increasing knowledge of data rights, which might include access, portability, and informed consent information. The dissemination of information to citizens regarding their rights and responsibilities is of the utmost importance as digital health technologies continue to transform. A great number of people continue to be ignorant of the rights that they have been granted by the GDPR or the repercussions of disclosing their health data. Partnerships between the government and educational institutions, non-governmental organizations (NGOs), and healthcare providers should be formed in order to include data literacy programs in more comprehensive health efforts.

There is a crucial junction of technical innovation, regulatory frameworks, and societal values in Finland, and it is represented by the management and ownership of health data. The healthcare system in Finland will need to be able to navigate a dynamic terrain by the year 2050. This landscape will be molded by developments in artificial intelligence (AI), wearable health devices, and data-driven decision-making, in addition to the ever-evolving needs of privacy, security, and equity. Through the course of this thesis, we have investigated the ways in which the General Data Protection Regulation (GDPR), Finnish national laws, and developing technology trends have an impact on the governance of health data and provide potential avenues for the future.

Important findings highlight the necessity for precise legal definitions of ownership of health data, particularly in the case of data generated by smart devices and processed by AI systems. This is especially true in the world of artificial intelligence. When it comes to addressing the commercialization and interoperability of health data, Finland's legal framework, which includes the Act on the Secondary Use of Health and Social Data (552/2019) and the General Data Protection Regulation (GDPR), provides a solid

foundation; nonetheless, there are still holes in the system. Additionally, the utilization of MLP in the research demonstrated that effective governance necessitates the alignment of niche innovations, established regimes, and broader social forces.

Recommendations for changes such as clarifying ownership rights, developing robust governance structures for artificial intelligence, and improving interoperability frameworks are included in this thesis. These recommendations are intended to ensure the ethical and sustainable use of health data. By making these efforts, individual rights, innovation, and the benefits to society will be brought into balance.

By tackling these difficulties, Finland will be able to position itself as a global pioneer inequitable and privacy-centric health data governance, which will ensure both innovation and trust in healthcare systems by the year 2050. This is because Finland is striving to attain a leadership position in digital health.

References

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. 2016 2nd international conference on open and big data (OBD),

Ballantyne, A. J. J. o. m. e. (2020). How should we think about clinical data ownership? , *46*(5), 289-294.

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., . . . Dasgupta, D. J. J. o. m. s. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *44*, 1-9.

Contreras, J. L. J. N. R. (2019). The false promise of health data ownership. *94*, 635.

Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. J. J. o. b. d. (2019). Big data in healthcare: management, analysis and future prospects. *6*(1), 1-25.

Finland, S. (2015). Official statistics of Finland (OSF): population projection. In.

Geels, F. W., & Schot, J. J. R. p. (2007). Typology of sociotechnical transition pathways. *36*(3), 399-417.

Geels, F. W. J. E. i., & transitions, s. (2011). The multi-level perspective on sustainability transitions: Responses to seven criticisms. *1*(1), 24-40.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González., (2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Hatfield v. Straus, (82 N.E. 172, 176, N.Y. 1907).

Hoerbst, A., & Ammenwerth, E. J. M. o. i. i. m. (2010). Electronic health records. *49*(04), 320-336.

Hutchinson, T. (2013). Doctrinal research: researching the jury. In *Research methods in law* (pp. 15-41). Routledge.

Int'l News Serv. v. Associated Press, (248 U.S. 215, 235, 1918).

John, L. J. N. Y., USA: Blackmore Dennett. (2018). Second Treatise on Civil Government.

Khan, N. A., Brohi, S. N., & Zaman, N. J. A. P. (2023). Ten deadly cyber security threats amid COVID-19 pandemic.

Kremen vs Cohen, (9th Circuit Court 2003).

Kumar, S., Singh, M. J. B. d. m., & analytics. (2018). Big data analytics for healthcare industry: impact, applications, and tools. *2*(1), 48-57.

Liddell, K., Simon, D. A., Lucassen, A. J. J. o. L., & Biosciences, t. (2021). Patient data ownership: who owns your health? , *8*(2), lsab023.

Macpherson, C. B. (1962). The political theory of possessive individualism: Hobbes to Locke.

Mandel, J. C., Kreda, D. A., Mandl, K. D., Kohane, I. S., & Ramoni, R. B. J. J. o. t. A. M. I. A. (2016). SMART on FHIR: a standards-based, interoperable apps platform for electronic health records. *23*(5), 899-908.

Mantelero, A. J. C. L., & Review, S. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *34*(4), 754-772.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. J. B. (2017). Cybersecurity and healthcare: how safe are we? , *358*.

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. J. J. o. m. s. (2015). Privacy and security in mobile health apps: a review and recommendations. *39*, 1-8.

Maximilian Schrems v Facebook Ireland Limited., (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0498

McNally v. United States, (483 U.S. 350 1987).

Mirchev, M., Mircheva, I., & Kerekovska, A. J. J. o. M. I. R. (2020). The academic viewpoint on patient data ownership in the context of big data: scoping review. *22*(8), e22214.

Montgomery, K., Chester, J., & Kopp, K. J. J. o. I. P. (2018). Health wearables: ensuring fairness, preventing discrimination, and promoting equity in an emerging Internet-of-Things environment. *8*, 34-77.

Murray, F. J. A. J. o. s. (2010). The oncomouse that roared: Hybrid exchange strategies as a source of distinction at the boundary of overlapping institutions. *116*(2), 341-388.

O'Brien v. O'Brien, (489 N.E.2d 712, N.Y. 1985).

Ogundele, O., Isabirye, N., & Cilliers, L. (2018). A model to provide health services to hypertensive patients through the use of mobile health technology. Conference Proceedings of African Conference of Information and Communication Technology, Cape Town, South Africa,

Pateman, C. J. J. o. P. P. (2002). Self-ownership and property in the person: Democratization and a tale of two concepts. *10*(1), 20-53.

Payne v. Elliot, (54 Cal. 339, 342, 1880).

Piasecki, J., & Cheah, P. Y. J. B. M. E. (2022). Ownership of individual-level health data, data sharing, and data governance. *23*(1), 104.

Posner, R. A. J. L. R. (1978). The Right of Privacy, 12 Ga. *393*(41), 1.

Reddy, G. T., Reddy, M. P. K., Lakshmanna, K., Kaluri, R., Rajput, D. S., Srivastava, G., & Baker, T. J. I. A. (2020). Analysis of dimensionality reduction techniques on big data. *8*, 54776-54788.

Sainz-de-Abajo, B., de la Torre-Díez, I., Góngora-Alonso, S., & López-Coronado, M. (2020). Privacy issues in eHealth and mHealth apps. In *Health Data Privacy under the GDPR* (pp. 71-82). Routledge.

Terry, S. F., Terry, P. F., Rauen, K. A., Uitto, J., & Bercovitch, L. G. J. N. R. G. (2007). Advocacy groups as research organizations: the PXE International example. *8*(2), 157-164.

Testa, S. (2022). An Overview of the Secondary Use of Health Data Within the European Union: EU-Driven Possibilities and Civil Society Initiatives. Privacy Symposium: Data Protection Law International Convergence and Compliance with Innovative Technologies,

Tikkinen-Piri, C., Rohunen, A., Markkula, J. J. C. L., & Review, S. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *34*(1), 134-153.

Topol, E. J. J. N. m. (2019). High-performance medicine: the convergence of human and artificial intelligence. *25*(1), 44-56.

Town of Castle Rock v. Gonzales, (545 U.S. 748, 768 2005).

Tully, J. (1993). *An approach to political philosophy: Locke in contexts* (Vol. 25). Cambridge University Press.

United States v. Evans, (844 F.2d 36 2d Cir. 1988).

Van Hoecke, M. (2011). Legal doctrine: Which method (s) for what kind of discipline? In *Methodologies of legal research: which kind of method for what kind of discipline?* (pp. 1-18). Hart Publishing.

Wainwright R, D. F., Fertik M, Rake M, Savage SC, Cloppinger JH. (June 8-9, 2011). *Personal Data: The 'New Oil' Of The 21st Century Presented in World Economic Forum on Europe and Central Asia*

World Economic Forum. Retrieved 22 April 2024 from https://www.weforum.org/publications/world-economic-forum-europe-and-central-asia-2011/

Wang, J., Zhang, Z., Xu, K., Yin, Y., Guo, P. J. I. J. o. S., & Applications, I. (2013). A research on security and privacy issues for patient related data in medical organization system. *7*(4), 287-298.

Westin, A. F. J. W., & Freedom. (1967). Privacy and Freedom London: Bodley head.