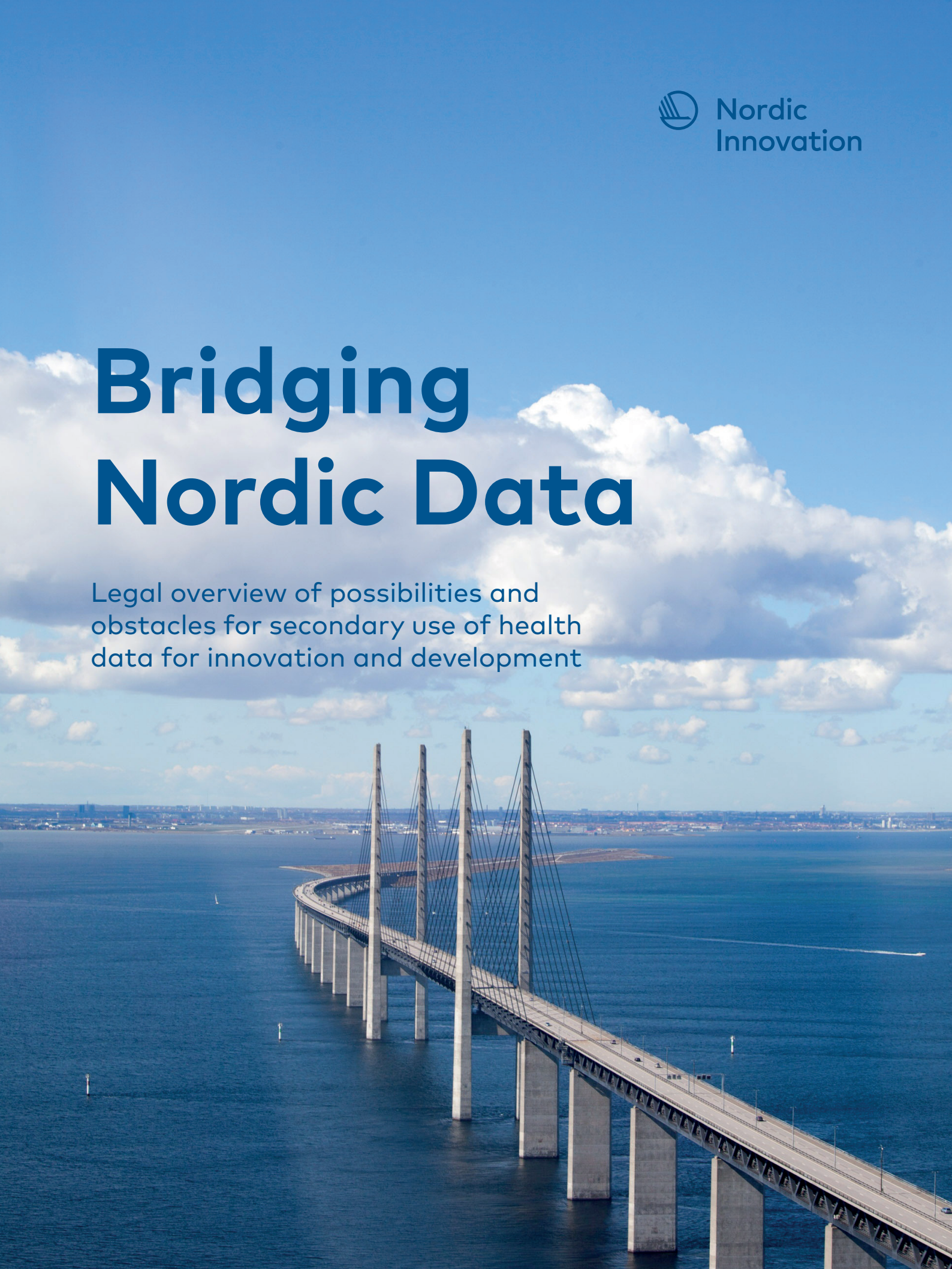
Nordic Innovation

Bridging Nordic Data

Legal overview of possibilities and obstacles for secondary use of health data for innovation and development



Bridging Nordic Data

© 2020 Nordic Innovation

Cover photo: pxhere.com

ISBN (print): 978-82-8277-112-2
ISBN (digital): 978-82-8277-113-9

Authored by Deloitte Legal for Nordic Innovation. The authors are responsible for the content of this report.

Deloitte.
Legal

Deloitte AS and Deloitte Advokatfirma AS are the Norwegian affiliates of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.no for a more detailed description of DTTL and its member firms.

Deloitte Norway conducts business through two legally separate and independent limited liability companies; Deloitte AS, providing audit, consulting, financial advisory and risk management services, and Deloitte Advokatfirma AS, providing tax and legal services.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's 312,000 people make an impact that matters at www.deloitte.no.

The future of health care is data driven

Nordic Health, Demography and Quality of Life is one of the main focus areas at Nordic Innovation and is based on the priorities of the Nordic ministers of business.

With the **Health, Demography and Quality of Life** program, we connect people, data and innovation for a better life – and help make the Nordics the most sustainable and integrated health region in the world, providing the best possible personalized health care for all its citizens.

With this program we hope to:

1. Help the Nordic region become a global test region and role model for sharing health data.
2. Establish collaboration platforms and connections between local ecosystems in the Nordics and potentially interesting global marked to increase Nordic export and competitiveness.
3. Contribute to develop better and more efficient health systems and increase health and welfare in the Nordic region.

We believe that the use and exploitation of health data will play a crucial role in our journey towards a more sustainable healthcare that will benefit Nordic citizens and businesses.

On assignment from Nordic Innovation, Deloitte Legal has carried out this legal overview of possibilities and obstacles for secondary use of health data for innovation and development. This report seeks to identify and assess the most relevant legal obstacles likely to hinder innovation and development activities across the Nordic region, as well as to provide an overview of legal barriers that the Nordic region must address jointly. Furthermore, existing possibilities for utilization of health data for innovation and development are identified with the objective of facilitating the flow of data across the region.

We would like to extend a special thanks to the members of the reference group (see page 102) for their valuable input during workshops and throughout the work with this analysis.

In addition to being a thorough source of information for Nordic Innovation and our partners, we hope the report will encourage decision makers, businesses and relevant actors in the health and welfare sector to take an active role in further exploring the possibilities for sharing and using health data in the Nordic region.

We have a unique possibility to become a global role model for sharing health data to benefit both citizens and businesses – let us make the most of it.

Oslo, June, 2020

Svein Berg
Managing Director, Nordic Innovation

TABLE OF CONTENTS

1. Preface 6

1.1 Background 6
1.2 Objective and scope 6
1.3 Methodology overview 7

2. Executive summary 8

3. Introduction 10

4. The General Data Protection Regulation (GDPR) 11

4.1 Introduction 11
4.2 Personal data, anonymous data and synthetic data 11
4.3 Lawful processing of health data 14
4.4 Regulation of scientific research in the GDPR 17
4.5 Rights of the data subject 18
4.6 Obligations of the controller 18
4.7 Transfer of and transborder access to personal data 20

5. Denmark 21

5.1 Introduction 21
5.2 Danish health care system and information resources 21
5.3 Legal reforms enabling secondary use 22
5.4 General principles on use of health data 22
5.5 Legislation 23
5.6 Access to health data for secondary use 25
5.7 Transfer of and transborder access to health data 31
5.8 National obstacles 32

6. The Faroe Islands 33

6.1 Introduction 33
6.2 Faroese health care system and information resources 33
6.3 Legal reforms enabling secondary use 33
6.4 General principles on use of health data 34
6.5 Legislation 34
6.6 Access to health data for secondary use 36
6.7 Transfer of and transborder access to health data 39
6.8 National obstacles 40

7. Greenland 41

7.1 Introduction 41
7.2 Greenlandic health care system and information resources 41
7.3 Legal reforms enabling secondary use 41
7.4 General principles on use of health data 42
7.5 Legislation 42
7.6 Access to health data for secondary use 44
7.7 Transfer of and transborder access to health data 47
7.8 National obstacles 47

8. Finland 49

8.1 Introduction 49
8.2 Finnish social and health care system and information resources 49
8.3 General principles on use of health and social data 51
8.4 Legislation 52
8.5 Transfer of and transborder access to social and health data 58
8.6 National obstacles 59

9. Åland **60**

10. Iceland **61**

10.1 Introduction 61
10.2 Icelandic health care system and information resources 61
10.3 Legal reforms enabling secondary use 62
10.4 General principles on use of health data 63
10.5 Legislation 64
10.6 Access to health data for secondary use 66
10.7 Transfer of and transborder access to health data 71
10.8 National obstacles 72

11. Norway **73**

11.1 Introduction 73
11.2 Norwegian health care system and information resources 73
11.3 Legal reforms enabling secondary use 73
11.4 General principles on use of health data 74
11.5 Legislation 75
11.6 General regulation on health research 75
11.7 Access to health data for secondary use 77
11.8 Transfer of and transborder access to health data 83
11.9 National obstacles 83

12. Sweden **84**

12.1 Introduction 84
12.2 Swedish health care system and information resources 84
12.3 Legal reforms enabling secondary use 85
12.4 Legislation 85
12.5 Access to health data for secondary use 87
12.6 Transfer of and transborder access to health data 92
12.7 National obstacles 93

13. Use of health data across the Nordics **94**

13.1 General 94
13.2 Possibilities under existing legislation 94
13.3 Main obstacles under existing legislation 96
13.4 Final remarks 100

14. Appendices to the report **102**

14.1 Appendix 1 - Members of Reference Group 102
14.2 Appendix 2: Relevant definitions from the GDPR 102

Figure 1 - The privacy principles 14

Figure 2 - Alternative legal bases in the GDPR 16

Figure 3 - Regulated division of primary and secondary use of health data in Denmark 31

Figure 4 - Regulated division of primary and secondary use of health data in the Faroe Islands 39

Figure 5 - Regulated division of primary and secondary use of health data in Greenland 47

Figure 6 - Regulated division of primary and secondary use of health and social data in Finland 50

Figure 7 - The Finnish process for acquiring health and social data for secondary use 52

Figure 8 - Regulated division of primary and secondary use of health data in Iceland 70

Figure 9 - Regulated division of primary and secondary use of health data in Norway 82

Figure 10 - Regulated division of primary and secondary use of health data in Sweden 92

1. Preface

1.1 Background

The Nordic Innovation (NI) program Health, Demography and Quality of Life was launched 1 January 2018, aimed at advancing the Nordic region to be the most sustainable and integrated health region in the world by 2030. The program is based on the priorities of the Nordic ministers for business, as outlined in the Nordic Co-operation Programme for Business and Innovation Policy 2018-2021.[1] Through four action areas relating to sharing of health and personal data, shifting focus from treatment to prevention, creating a healthy supportive environment, and utilizing the full innovation potential for the Nordics and beyond, NI believes that the Nordics will be able to provide the best personalized health care for all Nordic citizens.[2]

The first action area and the focus of this report is called the Bridging Nordic Data Initiative. The initiative aims at increasing innovation in public and private sectors through increasing possibilities for utilization of health data across the Nordic borders. Through efficient sharing and use of such information, to provide patients with better and more personalized health care, as well as achieve a more patient centered approach is presumed possible.

As part of the initiative, NI sent an invitation for tender 22 October 2019, seeking to purchase an overview of the main obstacles and practices within the field of health data in the Nordic region. Deloitte Legal is the supplier of the assignment.

1.2 Objective and scope

To achieve the vision of the initiative and to utilize health data across the Nordic region, fluent circulation of health data between relevant actors within the health sector is considered necessary. The Nordic region, which for the purpose of this report includes Denmark, Finland, Iceland, Norway, Sweden, Greenland, the Faroe Islands, and Åland, is recognized for having societal similarities, in which the spirit of voluntary communal work and the citizens reliance in the authorities are prominent characteristics. There is a long tradition for co-operation between the five countries and three self governing territories, also in respect to legislative changes.

The official co-operation in the Nordic region take place within the scope of the Nordic Council of Ministers and the Nordic Council, which aims at making the Nordic region the most sustainable and integrated region of the world.[3] Due to the significant societal and legislative similarities within the Nordic region, the basis for achieving fluent circulation of health data appears promising. However, due to strict health regulations throughout the Nordic region, amendments to the existing legal environment is assumed necessary to achieve the intended goal. This report seeks to identify and assess the most relevant legal obstacles likely to hinder innovation and development activities across the Nordic region, as well as to provide an overview of legal barriers that the Nordic region must address jointly. The report also seeks to identify and assess existing possibilities to utilize health data for innovation and development purposes.

Innovation and development are considered secondary use purposes. Primary use refers to use in which the data primarily was collected for, while secondary use refers to the use of data for other purposes. In connection to health data, primary use typically refers to provision of treatment and health care to the data subject. Assessment of regulation on transborder access to health data for primary purposes are outside of scope.

The focus of this report is the use of health data for innovation and development purposes. Other secondary use purposes, such as scientific research and statistics, are in principle outside of scope. However, as the terms innovation and development and scientific research intertwine, it is not always possible to differentiate between the terms.

Apart from in Finland, innovation and development specific regulation is near absent in Nordic legislation. Further, there are no general definitions of the terms innovation and development, or scientific research. From a legislator's point of view, it appears that scientific research generally is understood as basic research and applied research. According to the Organization for Economic Cooperation and Development (OECD), the term 'innovation' is understood as "*... the implementation of a new or significantly improved product (good or service), or process... or a new organisational method in business practices, work-place organisation or external relations.*" The term 'innovation activities' is further defined as "*... all scientific, technological, organisational, financial and commercial steps which actually, or are*

[1] Norden Council of Ministers (2018): https://norden.diva-portal.org/smash/get/diva2:1175601/FULLTEXT01.pdf
[2] Please refer to the following site for details on the program: https://www.nordicinnovation.org/health
[3] Please refer to the following site for details on the vision: https://www.norden.org/no/deklarasjon/var-visjon-2030

intended to, lead to the implementation of innovations.... Innovation activities also include R&D that is not directly related to the development of a specific innovation." [4]

On the other hand, the term 'research and development' is understood by OECD to "...comprise creative and systematic work undertaken in order to increase the stock of knowledge...and to devise new applications of available knowledge". The term is further considered to include three activities; basic research, applied research, and experimental development, in which experimental development is understood as "...systematic work, drawing on knowledge gained from research and practical experience and producing additional knowledge, which is directed to producing new products or processes or to improving existing products or processes".[5]

As shown by the understandings of OECD, there are a close relationship between innovation, research and development. Innovation may be research-driven to a greater or lesser extent, and may result from research, hereunder experimental development or other activities not performed by the innovation business itself. For these reasons, national regulation allowing access to health data for scientific research will be addressed when deemed necessary. Ways of including innovation in clinical practices, as requirements for clinical trials involving humans and requirements for medical devices, will not be addressed in the following, neither the relationship between scientific health research and the provision of health care.[6]

As this report will provide an overview of relevant obstacles under existing legislation, any thorough assessment of how to overcome these challenges and the consequences of doing so are not included. For this reason, this report should be supplemented by findings in other published reports regarding secondary use of health data in the Nordics.

1.3 Methodology overview

This report is written by Deloitte Legal, represented by Deloitte Statsautoriseret Revisionspartnerselskab (Deloitte Denmark), Deloitte Oy (Deloitte Finland), Deloitte ehf. (Deloitte Iceland), Deloitte Advokatfirma AS (Deloitte Norway), and Deloitte AB (Deloitte Sweden). The respective firms are responsible for the separate country specific chapter. In addition, Deloitte Denmark is responsible for the chapters on the Faroe Islands and Greenland, and Finland is responsible for the chapter on Åland. Deloitte Norway holds the administrative and coordinative responsibility.

The representatives from each country have worked collectively to prepare a report outline to reflect both relevant national possibilities and obstacles for processing health data for innovative and development purposes. To provide a clearer understanding of the assignment and the objective, NI hosted an introductory workshop, where a reference group set up by NI and Deloitte Norway participated. Please refer to Appendix 1 for the full list of the reference group members.

Each country has performed a thorough review of national legislation applicable to the field of data privacy and health care. The findings have been analyzed based on traditional legal methodology. When deemed necessary to obtain a nuanced understanding of the legal framework and practices, relevant authorities and stakeholders have been contacted by Deloitte Legal. In this regard, some of the members in the reference group and other relevant market actors have been contacted by Deloitte Legal by phone or email.

Based on the country specific findings, a comparative analysis has been conducted to identify possibilities and obstacles for utilization of health data for innovation purposes applicable throughout the Nordic region.

Please note that unofficial translations of national legislation and other sources have been used. In case of any discrepancy between the national and translated versions, the national versions shall prevail.

Further, this report is based on legislations of eight different countries. Although homologous translations of wordings and phrases have been attempted, reservations are made with regards to nuances made in the comparative section of this report.

[4] Oslo Manual, Guidelines for Collecting and Interpreting Innovation Data, 3rd Edition, OECD (2005).
[5] Frascati Manual 2015 Guidelines for Collecting and Reporting Data on Research and Experimental Development, OECD.
[6] The use of Artificial intelligence (AI), e.g. machine learning, challenge the clear legal distinction between conduction of scientific health research and the provision of health care, Kunstig Intelligens og norske helsedata, Teknologirådet (2019).

2. Executive summary

The consensus amongst market actors in the health sector is that health data is of great value for future research, innovation and development. Digital development widens the range of use and ways of generating health data, such as through applications, wearables and similar devices. Access to health data is a prerequisite for the success of innovation and development projects. However, access to health data can be problematic. The Nordic region, consisting of Denmark, Finland, Iceland, Norway, Sweden, the Faroe Islands, Greenland, and Åland is known for having similar legislative framework, shared values and a long tradition for governmental co-operation. Across the Nordic region, health data is regarded sensitive of nature it is protected by strict professional secrecy. Therefore, access by disregarding professional secrecy is dependent on a legal basis. The picture is further complicated as provisions disregarding professional secrecy not necessarily are considered legal basis for subsequent processing of data under the GDPR.

Although health data is strictly regulated across the Nordics, certain common possibilities for accessing and processing health data for the purposes of innovation and development exist:

- Firstly, consent is recognized as a legal basis for processing of health data, regardless of the purpose of processing. Although consent can be considered a reliable and simple method of obtaining a legal basis, it introduces certain challenges for innovators as for researchers. From an innovator's perspective, the difficulties are primarily connected to preparing a consent precise enough to comprise the innovative activities in question, as such projects can evolve quickly and change over the course of the project. In addition, obtaining consent can be time-consuming and the risk of an inadequate number of participants is of great relevance. Further, there is a risk of consents being withdrawn, resulting in deletion of data and consequential deficient data sets unless anonymized. Additional considerations must also be taken, such as method of collection, procedures for review and withdrawal, and how to demonstrate compliance with the scope of consent. Consequently, consent is not always a suited legal basis for innovative activities.
- Secondly, alternative legal bases, not requiring the data subjects' consent, can be regulated by law. Finland has advanced compared to the other countries and self governing territories in the Nordic region, being the only country with specific regulation for processing health data for innovative and development purposes. One of the objectives of the newly introduced regulation is to facilitate for innovation and development activities, in which Finland succeeds. However, as health and social data can only be obtained in form of aggregated statistics for development and innovation purposes, the variability and usability of available data is somewhat limited. For access to non-anonymized data, an innovator must rely on an alternative legal basis for other secondary purposes under national legislation. In the other countries and self governing territories in Nordic region, legislation concerning innovation and development are near absent. Thus, an innovator must always rely on a legal basis for other secondary purposes under national law. Across the Nordics, examples of such alternative bases for secondary use are for scientific research, statistics, health analysis and quality assurance. Normally, the exception applicable for innovation purposes is for scientific research. The main challenge connected to alternative legal bases is to determine the area of application.
- Thirdly, an option is to use anonymized data for the purpose of an innovative project. In contrast to health data, anonymized data is not subject to the GDPR or other data protection legislation. Thus, professional secrecy can generally be disregarded. However, as anonymization itself requires a legal basis, anonymization introduces certain challenges. The anonymization process can be time-consuming, and some health data is unsuitable for anonymization or cannot be anonymized. In addition, it can be cumbersome to use anonymized data as it is does not provide the possibility of follow up conversations or questions to obtain necessary clarifications from participants.
- Fourthly, user generated data may be used as an alternative to health data. As mentioned above, technological development in society has provided the opportunity for generating health data through other means than provision of health care. As user generated health data is generally not subject to professional secrecy, processing of such data is less complex and often regulated by the data subject consent or agreement. Such data can also easily be transferred, increasing usability.
- Regarding transfer of health data across national borders, few additional limitations apply compared to domestic processing. Transfer of health data is generally regulated by the GDPR, which principles applies across the Nordic region except for the Faroe Islands and Greenland. Thus, certain additional requirements may apply for transfer to or from these countries. In addition, e.g. in Finland, foreigners have

limited access to health data, as a national identification code is required to submit a request or application for access.

Although there are some general possibilities for accessing and processing health data in the Nordic region, certain legal obstacles complicating the process of transferring health data apply. In addition to certain country specific obstacles, four general obstacles have been identified:

- Firstly, apart from in Finland, it is evident that the lack of innovation specific regulation constitutes a significant obstacle for innovation and development activities across the Nordics. In general, processing health data for such purposes is reliant on the data subjects' consent. As mentioned above, the most relevant alternative to consent as legal basis is the legal exception for scientific research, introducing the challenge of distinguishing scientific research from innovation and development. Bearing this challenge in mind, in practice it is demanding to decide upon the scope of these exceptions. A conceptual distinction between scientific research and innovation is that scientific research aims at creating new knowledge, while innovation is aimed at applying already existing knowledge. Due to the close relationship and lack of a regulatory clarified line between the terms, relevant authorities are left with a great amount of freedom when assessing whether permission for access and subsequent processing should be granted or not. For an innovator, it can be difficult to ascertain the conditions for access, and the process under existing legislation appear both costly and uncertain. In this regard, Finland has advanced compared to the other countries and self governing territories in the Nordic region, as processing for innovation specific purposes are explicitly regulated. As mentioned above, a downside to the regulation is that it applies to aggregated data only. For processing of health data, the legal limitations are similar across Nordic region.
- Secondly, the process of accessing health data is further complicated by decentralized information structures. Health data is stored in multiple information structures, such as in medical records, national health registers, national archives and biobanks, often regulated by different legislations, managed by different data controllers or registry keepers, and supervised by different authorities. Access procedures vary based on the type of health data and the above mentioned factors, making it difficult to gain full overview and increases cost of the process due to reliance on independent consultants. Lack of an organized scheme or method for accessing health data presents a risk of valuable data not being identified nor included in a data set requested for an innovation project. Although there have been several initiatives to establish centralized systems for access to and storage of health data, there are no fully centralized solutions established at the time of this report, neither on a Nordic nor on a national level. Finland has progressed the furthest by establishing Findata, an authority that collects, processes and provides access to data.
- Further, in close connection to the previous obstacle, additional permit requirements often apply for specific purposes of use. E.g. in Denmark, additional permit requirement typically from a scientific ethics committee is required for access for scientific research purposes. Similar additional requirements apply for the other countries and self governing territories in the Nordic region. In this regard, Finland differ from the other countries and self governing territories in the Nordic region by establishment of the authority Findata, which serves as a single point of access to health data.
- The fourth and final obstacle on a general level, though more practical than legal, relates to lack of standardization and interoperability. As health data, especially in medical records, is recorded using different technical systems and practices, it can be difficult to identify and collect all health data required for a predefined purpose. Although Finland and Denmark have advanced in terms of electronic keeping of health data, the lack of standardization and interoperability poses as a challenge from an innovator's perspective. This applies both on a Nordic and a national level.

To summarize, specific challenges must be addressed to facilitate for innovation and development across the Nordic region. The first and most significant action point is to explicitly address innovation and development in established legislation because it will contribute to a clearer picture of when access and processing is permitted for innovation and development purposes, as well as avoid the assessment of any differences between research and development, which up until now has been a source of inconvenience. Subsequently, as recognized by several market actors in the health sector, establishment of centralized systems, standardized procedures and both regulatory sandboxes and data sandboxes for health data will presumably contribute to increased and seamless transfers of health data across the Nordic region.

3. Introduction

The global health care sector is rapidly transforming. Advanced technological solutions, new and joint sources of data, the introduction of various health applications, and an increased focus on patient centered solutions indicates that the future of health care is data driven. Use of Artificial Intelligence (AI) has progressed from theory to practice, and everyday life has become intertwined with the Internet of Medical Things (IoMT).[7] Processing health and personal data is essential for the success of such digital solutions.

Although the use of digital solutions within the health care sector is increasing, several reports emphasize that further advancement is hindered by the existing legal framework. Health data is considered a special category of personal data under the GDPR and is subject to strict privacy rules. Thus, the possibilities to generate, access and process health data is limited.

As described by Wilkinson regarding research, which also applies for innovation, health data must be findable, accessible, interoperable and reusable (the FAIR-principles).[8] As further described in this report, anonymized data concerning health is not subject to the GDPR and can be used more freely. To facilitate development of innovative solutions to remedy pressing issues within health care, easy and lawful access to health data is necessary.

Recent development show that the legal environment is changing slowly. Several reports stress the need for legal amendments to facilitate for digital solutions and innovation, including within the area of health law. As an example, the European Commission is working on a digital transformation, aimed at establishing interconnected market for sharing personal data within the EU.[9] Particularly, it is emphasized that compared to larger corporations, small and medium enterprises (SMEs) do not have the same premise for accessing health data and to a limited extent have utilized digital solutions resulting in missed expansion opportunities. Especially diverging national legislation increasing administrative burdens has influenced this outcome. Another example can be found in the U.S., where rules providing patients with more control over health data has been introduced.[10] The new rules facilitate for easier access to health data by third parties, as well as restricting opportunities to refuse exchange of health data, including health data protected by professional secrecy. The new rules are intended to increase innovation and competition, as well as promote transparency using modern and digital solutions.

As new digital solutions utilizing health data continuously are developed, the need for special regulation for innovation and use of anonymized health data is increasing. In connection to the recent Covid-19 pandemic, several applications and electronic solutions for infection tracking and control have been hastily developed, most of which involving use of health data. It is evident that several of these solutions experience challenges due to existing legislation. Thus, although several Nordic policy documents and reports emphasize the future health advantages of the Nordic region resulting from shared values, similar legislation, and extensive collection of health data in registries, medical records, and through health surveys, further progress may be limited by both technological and national legal barriers.

In the following chapters, a legal overview of the existing legislative framework within the area of health in the Nordic region is presented. As the GDPR affects national legislation in the Nordic region to a greater or lesser extent, chapter 4 includes the principles for access to personal data and health data under the GDPR. The following chapters 5 to 12 are country specific, each presenting a legal overview of the procedures for accessing and processing health data under existing national legislation. Finally, chapter 13 presents a comparative analysis aimed at emphasizing the possibilities and obstacles for accessing and processing of health data for innovation and development purposes across the Nordic region.

[7] Describes the infrastructure of all medical devices: https://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things

[8] FAIR Data Principles, Wilkinson, M. D. et al. (2016).

[9] European Commission (2020), https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[10] The 21st Century Cures Act (85 FR 25642): Interoperability, Information Blocking, and the ONC Health IT Certification Program and Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers (CMS-9115-F). The rules will be effective on effective on June 30, 2020.

4. The General Data Protection Regulation (GDPR)

4.1 Introduction

Privacy and data protection are regarded fundamental rights within the European Union (EU) and the European Economic Area (EEA).[11] Individuals have the right of protection of their personal data, and personal data shall only be used in a fair and lawful way in line with the principles of the GDPR. To utilize health data, the national data protection legislation must be complied with. The GDPR is a general set of rules, which applies regardless of specific provisions in national health legislation. Thus, innovators and developers operating within the scope of the GDPR must comply with the GDPR requirements on use of health data. The GDPR is applicable in Denmark, Finland, Iceland, Norway and Åland. Although the GDPR is not directly applicable in the self governing areas of Greenland and the Faroe Islands, the data privacy legislation is based on the GDPR. Thus, to utilize health data in and from the Nordic region, knowledge of the requirements of the GDPR is of particular relevance.

Through the implementation of the GDPR, individual's data protection and ownership to own data is strengthened. Processing of personal data must be based on the principles set forth in the GDPR, in which the processing must be considered legal, transparent, and fair. Data can only be processed for specific purposes and must be limited to what is considered necessary for the purpose of use. After the purpose of use is achieved, all personal data must be deleted. The GDPR imposes administrative fines for non-compliance, and infringements may lead to administrative fines up to EUR 20 000 000 or up to 4 per cent of the total annual turnover.[12] Both controllers and processors of personal data can be subject to such fines. In the following, relevant clarifications and basic principles for processing of personal data under the GDPR, are presented.

4.2 Personal data, anonymous data and synthetic data

4.2.1 Personal data

To assess whether an innovator is obliged to comply with the GDPR, the meaning of the term personal data must be understood. As explained below, health data is a special category of personal data.

Personal data covers any information that can be related to an identified or identifiable natural person, referred to as the data subject.[13] Thus, the term personal data is generally interpreted broadly.[14] Where a natural person can be identified, directly or indirectly, through different factors such as a name, an identification number, location data, an online identity etc., the data is regarded as personal data. Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person can also be regarded as personal data in this context, but only if they contribute to the identification of an individual. Whenever such data is linked to a direct identifier, all the connected data will be regarded as personal data in that context.[15]

The GDPR does not apply to the processing of personal data of deceased persons, but Member States may provide for such rules in national legislation.[16]

Pseudonymized data is personal data, which due to processing, no longer can be attributed to a specific data subject without the use of additional information, an identification key. To be regarded as pseudonymized data, the identification key must be kept separate and be subject to measures ensuring that the personal data cannot be linked to the data subject.[17]

This means that pseudonymized health information can constitute health data for a health care provider or agency holding the identification key, however be considered anonymous for an external party with no legal or practical access to such key of identification. Pseudonymized data is still classified as personal data and the GDPR applies, however often subject to more lenient regulation.

4.2.2 Anonymous data

Anonymous data is information unrelated to an identified or identifiable person. As the GDPR only applies to personal data, the processing of anonymous data is not regulated by the GDPR.[18] Consequently, data which is

[11] C.f. e.g. the Universal Declaration of Human Rights 1948 (UDHR) article 48; EMK article 8; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); and ECHR article 8.
[12] Cf. the GDPR article 83.
[13] Ibid. article 4 (1).
[14] Stated by the European Court of Justice in several decisions: https://gdpr-info.eu/issues/personal-data/
[15] Cf. the GDPR recital 26.
[16] Ibid. recital 27.
[17] Cf. the GDPR article 4 (5).
[18] Ibid. article 4 (1).

considered anonymous may for example be collected, registered, transferred and stored without limitations.

Access to data is a prerequisite for the digital economy. As a free flow of non-personal data is a prerequisite for a competitive data economy within the Digital Single Market, the EU has also adopted a regulation on free flow of non-personal data.[19]

Anonymous data is not regulated by the GDPR.

Personal data rendered anonymous so that the data subject no longer is identifiable, directly or indirectly, is equivalent to anonymous data.[20] Although medical records contain personal data, aggregated personal data from multiple medical records without any identification keys will in general not be considered personal data.

The concept of anonymous data is challenging. According to the GDPR's definition, an anonymized data set is a data set where all personal identifiable information is permanently removed. In practice, data can be deanonymized in several ways.[21] New research has showed that the existing methods for anonymizing data leave individuals at risk of being re-identified.[22] To determine whether a person is identifiable, one must consider all means likely to be used to identify the natural person. Because the classification impacts whether the GDPR applies, an innovator must be aware that *"means reasonable likely to be used"*, will differ over time, as technology evolves. How much time, effort and money it will take to de-anonymize the data must also be taken into consideration.

An alternative to anonymous data is synthetic data. Synthetic data is often described as a subset of anonymous data, although a synthetic data set is constructed and not a data set which originally contained personal data. Synthetic data is constructed to correspond to production data and is often used for testing purposes. The use of production data, including personal data, for testing purposes will often be in breach of the GDPR's principle of purpose limitation.

4.2.3 Health data

Health data is data directly or indirectly related to the physical or mental health of a person.

Health data is a special category of personal data.[23] If an innovator uses personal data related to the physical or mental health of a natural person, the processing includes health data.[24] Anonymous data will never be regarded as health data in this respect.

Compared to other types of personal data, health data is subject to firmer regulations. This also applies to data on health care services that indirectly reveals information about the individual's health status, as well as genetic data. Genetic data is personal data related to the inherited or acquired genetic characteristics of a natural person. Such data provides unique information about the person's physiology or health and will often derive from a biological sample analysis of the natural person in question.[25]

The GDPR defines health data in a broadly and includes any personal data revealing information about a person's health or health status, regardless of where the data has been collected from, such as the health care sector, wearables, or social media.

Further, data without a person's name or date of birth can be regarded as health data when it can be used to identify health attributes of a natural person. Examples are "*..a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test*".[26]

Consequently, if production data from a hospital not only reveals how many hospital beds that were used within a time period, but also may be connected to the hospitalized individuals the data set will contain personal data. On the contrary, a data set concerning only the number of used beds in a certain hospital within a specific time period will neither be personal data nor health data.

As technology develops, the definition of health data continuously changes. Thus, assumably information Spotify collects about individuals can be regarded as health data in the future. Even more so if the information is analyzed and used to predict aspects on an individual's

[19] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the EU.
[20] The GDPR recital 26.
[21] I.e. by cross-referencing certain facts or by connecting the data set with another and similar data set that has not been anonymized.
[22] Estimating the success of re-identifications in incomplete data sets using generative models, Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye (Nature, July 2019).
[23] In Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (the Data Protection Directive) these data were referred to as sensitive personal data.
[24] Cf. the GDPR article 4 (15).
[25] Ibid. article 4 (13).
[26] Ibid. recital 35.

mental health based on the type of music they listen to. The same may apply to data on individuals' behavior in social media.[27]

4.2.4 Basic principles innovators must meet when processing personal data

When processing health data as a part of an innovation project or any innovation activity innovators must comply with the basic principles for processing.[28] The controller is the one entity or natural person who decides on why and how personal data shall be processed.[29] An innovating SME may inherit this role when they alone, or jointly with others, make these decisions. The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.[30]

The controller's responsibility is absolute, also where the controller outsources the processing activities to a processor.[31] This means that if a hospital, as a controller is running an innovation project and uses a third party for technical development and the actual processing of personal data, the responsibility to demonstrate compliance with the data protection principles remains with the controller.[32] Same applies to a SME developing an app on its own. Before an innovation is brought to market, the company responsible for the development will be the controller of the personal data necessary to develop the app and present it to the market. Any subsequent processing of personal data when the app is used by a health care institution, will be within the responsibility of the institution in question. To be able to demonstrate compliance, the controller should maintain records and documentation of the processing activities including, but not limited to, what data is being processed and how, for what purpose and what security measures have been implemented. Usually this documentation should follow from and be stored in an internal control system.[33]

Personal data must only be collected for specified, explicit and legitimate purposes.[34] Likewise, innovators using health data must have a specific purpose for the usage. This may be challenging for innovation projects. As development proceeds the purpose may change. In another example, the main purpose of the usage may be to find any coherence between big data sets, without a hypothesis ready at point of data collection.

The principle of 'purpose limitation' sets a limiting legal frame as personal data cannot be further processed in a manner incompatible with the original purpose of use. Thus, in practice, health data processed to provide health care may only be processed for new purposes if there is a legal basis for continued processing. Health data processed as part of providing health care cannot be processed for innovation purposes, nor any other type of secondary use, unless there is a legal basis for this in the GDPR.[35] Regardless, the GDPR states that processing of health data for scientific research never is considered incompatible with the original purposes.[36] Thus, from an innovator's perspective, whether an innovation activity is within the scope of the definition of 'scientific research' is of significant importance, cf. this report section 4.4.

The innovator's use of personal data must be lawful, fair and transparent.[37] To be lawful, the way an innovator processes health data and other personal data must have a legal basis and be within one of the exceptions from the prohibition to process health data. If innovators can demonstrate that their work should be regarded as scientific research in the context of the GDPR, the use of health data will be lawful.[38]To be fair, there must be coherence between the processing and the purpose of the processing. The processing must also be deemed reasonable or fair to the data subject. The requirement of transparency means that the innovator's processing must be predictable for the data subject whose personal data is used in the project. This principle requires that any information and communication about the processing, must be easily accessible to the data subject, easy to understand, and in clear and plain language.[39]

When deciding upon which kind of personal data that should be used and will be needed as a part of the innovation activities, the principle of data minimization[40] must be upheld. The principle limits what and how much personal data may be processed for the specific purpose and require innovators to only process the data required. The use of personal data is only allowed where the purpose of the processing cannot reasonably be fulfilled by other means. Technology, like AI and machine learning, need large amounts of data to give useful answers. This may prove challenging when having the principle of data minimization in mind. Innovators should, when applicable, assess the possibilities of using less training data or to use anonymized data where possible to ensure the principle of data minimization.[41]

---

[27] Kunstig Intelligens og norske helsedata, Teknologirådet (2019)
[28] Ibid. article 5.
[29] Ibid. article 4 (7).
[30] Ibid. article 5 (2).
[31] Ibid. article 4 (8)
[32] Ibid. article 28.
[33] Many companies base their internal control system om international standards such as ISO 27001.
[34] Cf. the GDPR article 5 (1) b).
[35] Ibid. articles 6 and 9.
[36] Ibid. article 5 (1) b).
[37] Ibid. article 5 (1) a).
[38] Provided that there is a supplementary legal basis, cf. the GDPR article 92 j).
[39] The GDPR recital 39.
[40] Ibid. article 5 (1) c).
[41] TechGDPR (2019): https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/

As controller, the innovator must ensure that the personal data used is correct, relevant and that it is being updated when necessary.[42] The controller must take reasonable steps to ensure that appropriate processes are in place to ensure that the personal data is not incorrect or misleading.[43]

When personal data is processed, the data must be protected against unauthorized use, processing or change as well as against damage or destruction.[44] Both technical and organizational measures may be taken to protect the personal data.

Personal data cannot be kept longer than necessary to fulfil the purpose of the processing.[45] This means that innovators must delete data when the purpose of the processing is met. Automatic erasure within set frames is often seen as a good solution to ensure storage limitation. Exceptions to storage limitations are made for scientific research purposes.[46] The innovator, as a controller, decides upon the purpose when drafting an innovation project and must not forget to consider when this purpose will be regarded as fulfilled. This may be when the innovation is brought to market, hence the purpose is fulfilled, and the personal data must be deleted.

4.3 Lawful processing of health data

4.3.1 Alternative legal bases

If an innovator decides that health data is necessary to succeed in the innovation project, legal basis to process health data is required.[47] An innovator may have different roles going into an innovation or development project, being either a controller, joint controller or a processor.[48] The controller is responsible for the legal basis of the processing.

The GDPR provides alternative legal bases for processing, but not all of them will be a legitimate legal basis for secondary use of health data for innovation purposes.[49]

As health data is a special category of personal data, the processing of such data comes with a greater risk for the individuals concerned. Thus, processing of health data is generally prohibited. [50] However, the GDPR provides for exemptions allowing processing of health data.[51] Most of the exemptions, apart from the data subject's consent,

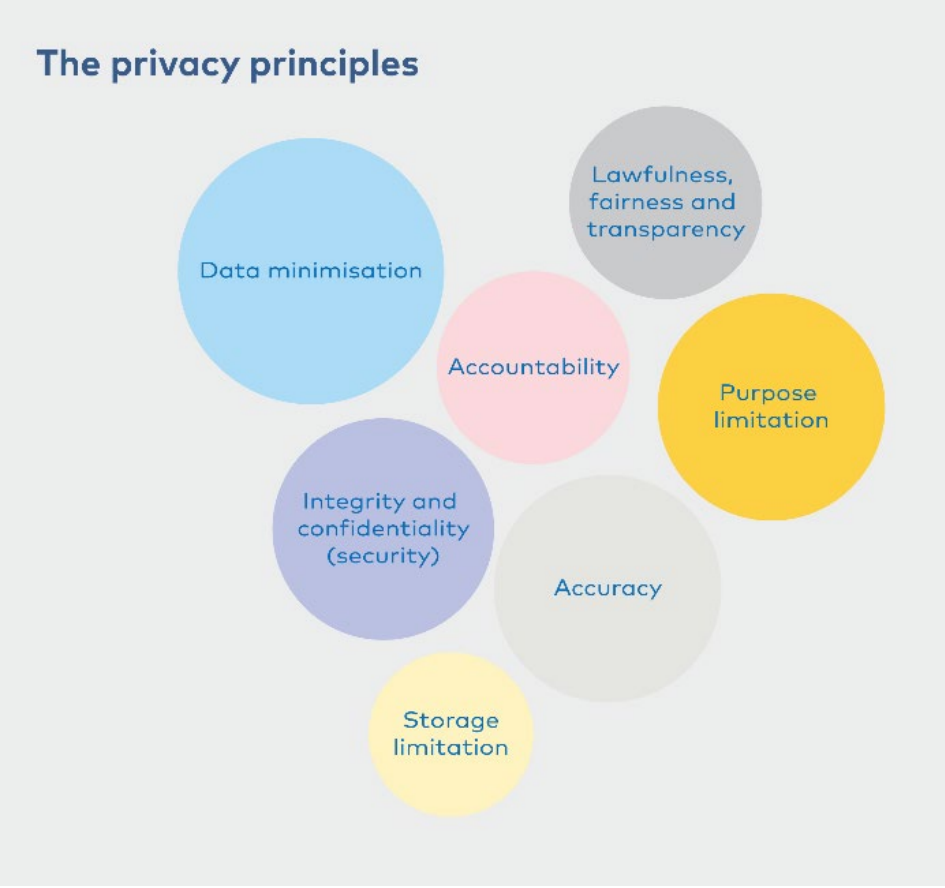


Figure 1 - The privacy principles

[42] The GDPR article 5 (1) d).
[43] In which case the controller may have an obligation to correct or erase the data cf. the GDPR article 17.
[44] The GDPR article 5 (1) f).
[45] Ibid. recital 3b).
[46] Ibid. article 5 (1) e), cf. article 89 (1).
[47] Ibid. articles 6 and 9.
[48] Ibid. articles 4 (7) and (8), article 26.
[49] Ibid. GDPR article 6.
[50] Ibid. article 9 (1).
[51] Ibid. article 9 (2).

may only be applied if the processing of health data is also regulated by national or EU law giving the processing a supplementary legal basis. Even if health data is needed to perform or enter into a contract with the data subject, one also need a separate exemption for processing this data.[52]

Without consent or a supplementary legal basis, health data may also be processed when it is in the vital interest of the data subject, typical if the processing is *"...essential for the life of the data subject or that of another natural person"*[53], hence it is rarely relevant for an innovation project.

Today, the most relevant and likely legal basis for innovation activities conducted in the Nordics, apart from in Finland, is consent from the data subject.[54] Alternatively, the processing of health data as a part of any innovation activity must be regulated national law, or the like, allowing processing of health data for any other purposes. The GDPR as such does not give any other legal basis relevant in this context. The country chapters will provide an overview of relevant legislation establishing the needed supplementary legal basis for the use of health data in innovation activities.

4.3.2 Consent

When processing personal data in relation to the development of health applications and health tech meant for personal use, processing based on the data subject's consent is the natural outset. This is also the most prominent legal basis when personal data is collected directly from the data subject in an innovation project with elements of scientific research. The same applies to processing of health data within the scope of automated decisions, i.e. decision made solely by the use of AI.[55] Consent will both constitute a legal basis for processing and provide an exemption from the ban on processing of health data as explained in this report section 4.3.1.

The data subject's consent[56] must fulfill certain requirements to serve as a legal basis;

- the consent must be provided from each data subject; and
- the consent must be specific, informed, unambiguous and requires an affirmative action.

The consent must be obtained before any data processing takes place and must be provided voluntarily, meaning that the data subject shall have a choice of rejecting that an innovator receives and processes the health data. This is particularly important if an innovator wants to use the health data for several purposes. In this case it is important that the data subject has the possibility to reject processing for any of the purposes.

The consent must be informed and limited to the necessary purposes. In other words, the data subject shall be precisely informed about which health data that will be processed and for which purposes[57], so the data subject knows exactly what the consequence of giving the consent is. The data subject must at least be provided with information about;

- the identity of the data controller;
- the purpose of the processing;
- which information that will be processed; and
- information about the right to withdraw the consent.

Further, it is important that the information is precise to the extent that the affirmative action of ticking a box, swiping, signing, etc. without doubt can be connected to the information. It is important to notice that an affirmative action is a precondition. Therefore, it is not enough to send an email to the data subject stating that if the data subject does not object, the data will be processed. The controller must be able to demonstrate that the data subject has consented. Innovators should at an early stage take into consideration how to document the consent.

> *There is a wide range of different health apps for smart phones, developed to promote behavior modification, to improve and monitor physical activity, or to remind patients to take medication.*
>
> *Such apps will in general need personal data in the developing phase and will generate personal data when used.*

Consent is also limited by the data subject's age. If a child is below the age of 16, consent must be given or authorized by the holder of the parental responsibility. The Member States may define a lower age limit, but not below 13.[58] Note that both Union or Member State law may prohibit the data subject from giving consent for the processing of health data.

The data subject can always withdraw any consent given. Despite a withdrawal, processing already done based on the consent is still valid. The withdrawal only concerns the lawfulness of the data processing after the withdrawal.

[52] Ibid. article 6 (1) b), cf. article 9 (1) cf. 9 (2).
[53] Ibid. recital 46.
[54] Cf. chapter 5-12.
[55] The GDPR article 22 cf. recital 71.
[56] Ibid. articles 4 (11) and 7, recital 32 and 42.
[57] Ibid. article 15.
[58] Ibid. article 8.

Upon withdrawal, personal data may be processed based on another legal basis, such as public interest as described below.

4.3.3 Reasons of public interest as legal basis

The GDPR states that health data should only be processed for health-related purposes when necessary to achieve purposes for the beneficial for both individuals and the society.[59] In this relation different health purposes are listed. The list covers, among others, management of health or social care services and systems, quality control, cross-border health care, health security, scientific and historical research and statistical purposes including studies.[60]

The Member States, as well as the EU, may by law or similar legislative measure allow processing of health data for reasons of public interest, as listed in the GDPR.[61] The legislative measure should be clear and precise, for the content to be evident for the data subject in question and provide suitable measures protecting the rights and interests of the data subject.[62] The measure should also be proportionate to the aim pursued. However, such measures should not impede the free flow of personal data within the EU when they apply to cross-border processing of health data.[63]

Thus, to assess whether the use of health data related to innovation activities may be based on another legal basis apart from consent, innovators must as a rule refer to national law.

To process personal data for research and statistics, additional safeguards are required, in particular to ensure data minimization, but the Member States may also exempt from some of the data subjects' rights.[64] The Nordic region already has in place several specific regulations on the processing of health data within the framework of these requirements, allowing processing of health data for different reasons of substantial public interest. Although, it seems that processing of health data for innovation as such in general is not included by these regulations.[65]

Processing necessary for the performance of a task carried out for reasons of substantial public interest may be allowed by law.[66] If the public interest is regarded as substantial, such legislation may both serve as a legal

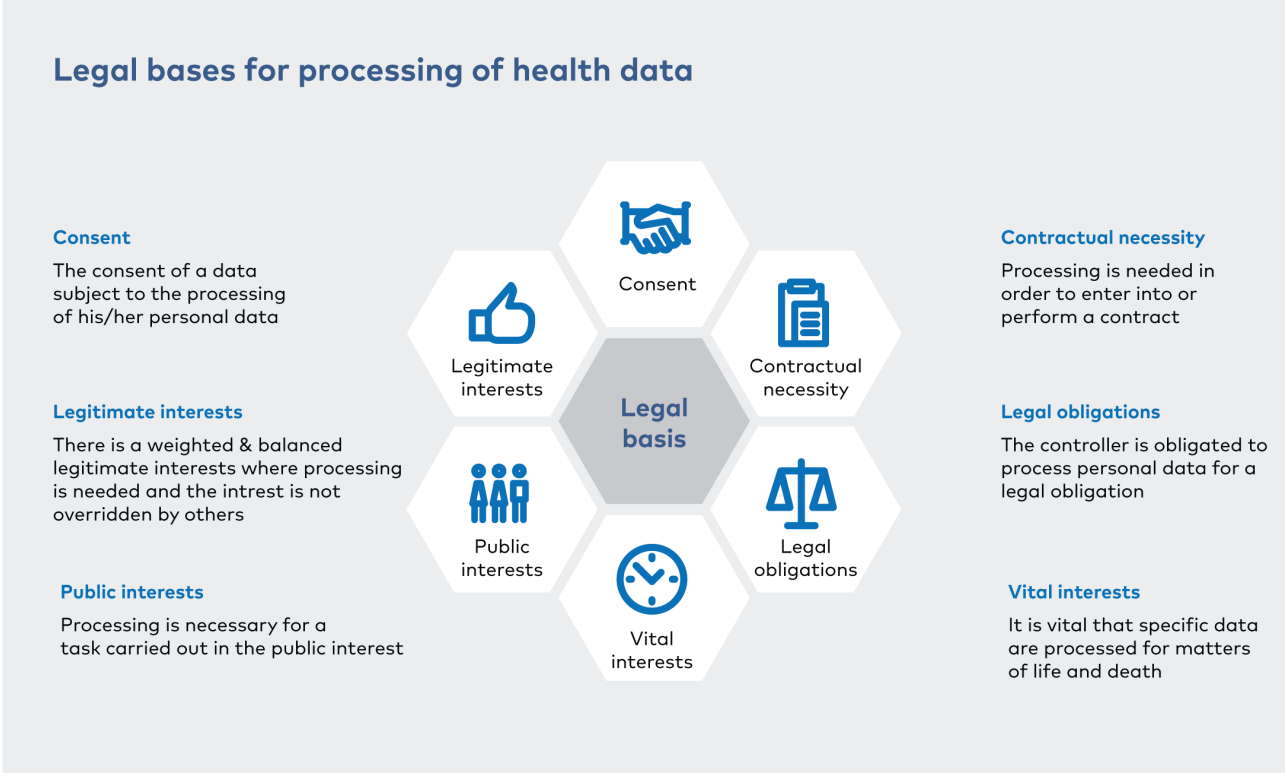


Figure 2 - Alternative legal bases in the GDPR

[59] Ibid. recital 53.
[60] Ibid. recital 53.
[61] Ibid. articles 6 and 9.
[62] Ibid. recital 41
[63] Ibid. recital 53.
[64] Ibid. article 89.
[65] Cf. chapter 5-12.
[66] The GDPR article 6 (1) e), cf. article 9 (2) g).

basis for the processing and an exemption from the prohibition of processing of health data. When assessing whether a purpose will constitute a substantial public interest one should look to the different purposes listed in the GDPR.[67]

For reasons of public interest in public health, processing of health data may also be granted by law. The latter may be both for protecting against serious cross-border threats to health or to ensure high standards of quality and safety of health care and of medicinal products.[68] As an example, the European Data Protection Board issued a statement in March 2020[69], emphasizing the possibility to process health data, when facing serious cross-border threats of epidemic character such as the COVID-19 virus. However, the derogation in the context of COVID-19 may be more relevant to public authorities.

Nevertheless, Member States may adopt legislative measures aimed at ensuring high standards of quality and safety of health care and of medicinal products, which could also cover processing of personal data in innovation activities.

Processing of health data necessary for scientific or historical research purposes or statistical purposes may also be allowed by law.[70] For processing of health data in research this is an important exemption.

4.4 Regulation of scientific research in the GDPR

The GDPR acknowledges the importance of scientific research and, to a certain extent, processing of personal data for this purpose is subject to less stringent regulations. To benefit from this, researchers must implement appropriate safeguards.[71]

When applying the GDPR, the processing of personal data for scientific research purposes should be interpreted in a broad manner and encompass both the public and private sector. The term is not defined in the GDPR, only described by various examples. Thus, the term "scientific research" will include for example technological development and demonstration, fundamental research, applied research and privately funded research.[72] Accordingly, innovation including an element of research will be regarded as scientific research in the context of the GDPR and may benefit from any special provisions in GDPR included to ease the processing of personal data for scientific research.[73]

The GDPR acknowledges researchers' need to combine health data from large populations from registries and other information sources to gain new knowledge of great value for the benefit of an improved health status in the society.[74] Thus, the Member States' possibility to facilitate scientific research within Member State Law are underlined. The Member States may also derogate from the data subjects' rights for this purpose.[75]

Innovators should especially note that further processing of personal data or health data collected for scientific research will not be incompatible with the original purpose.[76] For the purpose of research, the legislation also accepts that the data subject's consent is not based on detailed information but allowing data subjects to consent to their personal data being processed within certain areas of scientific research. This remedies the fact that scientific research for the most is not identified as a purpose of the processing at the time of collection[77] and gives research projects a wider possibility for secondary use of health data.

The GDPR also acknowledges researchers' need to store the data for a long time, thus the purpose of research in a way is exempted from the principle of storage limitation.[78]

Further, the GDPR allows researchers to transfer personal data to third countries outside EU/EEA that do not provide an adequate level of protection, although only in circumstances when the transfer is qualified as not repetitive and only concerns a limited number of data subjects.[79]

Based on this view, access to health data for mere innovation purposes are limited. Finland represents an exception in this regard, as innovation and development are explicitly distinguished from scientific research in their recently adopted Act on the Secondary Use of Health and Social Data, in which scientific methods are a requirement for something to be regarded as scientific research, cf. this report chapter 8. Due to lack of specific regulations in the other Nordic jurisdictions, secondary use for scientific research with an innovation perspective will be addressed when deemed necessary.

[67] Ibid. recital 53.
[68] Ibid. article 9 (2) i).
[69] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020 (Guidelines 04/2020, European Data protection Board)
[70] The GDPR Article 9 (2) j), cf. article 89.
[71] Ibid. articles 9 (2) j) and 89.
[72] Ibid. recital 159.
[73] Ibid. recital 33.
[74] Ibid. recital 157.
[75] Ibid. recital 156.
[76] Ibid. article 5 (1) b).
[77] Ibid. recital 33.
[78] Ibid. article 5 (1) e).
[79] Ibid. recital 113.

4.5 Rights of the data subject[80]

4.5.1 The right of access and information

The GDPR strengthens the protection of the individual's rights, and the individual's ownership to their own personal data. Awareness of these rights are specifically important when processing special categories of personal data as health data.

Innovators should note that the rights of the data subject include the right to be informed about the collection and the use of the data subjects personal data including, but is not limited to, information on what personal data is processed, how it is processed, by whom, if the controller intends to process the data for a purpose other than for which the personal data were collected[81], transfer of data to other controllers or to a third country or international organization.[82] The information must be available to the data subject in a concise, transparent, intelligible and easily accessible form, using a clear and plain language.[83] Such information is often made available to the data subject in a privacy statement found on the controller's web pages or made available for the data subject when giving consent.

Innovators who are controllers must facilitate a possibility for the data subject to access the data.[84] It is not a requirement that such access is digitalized, even though this may be the most practical solution.

4.5.2 The right to data portability

The GDPR introduced the right to data portability which entitles the data subject to request copies of their personal data in a readable and standardized format and transmit it to another controller.[85] Data portability only applies if the personal data concerned was provided by the individual to the controller, processed by automated means, and processed based on consent or fulfilment of a contract. Innovators of wearable technologies and smartphone apps aimed on voluntarily use by the data subject are obliged to provide the user generated personal data to the data subject in a structured machine-readable format. The data subject may use this right to transfer the same data to another health tech innovator or to a health care provider. The right to data portability is expected to foster opportunities for innovation.[86]

4.5.3 The right to object to automated decision-making

The data subject's right to object to automated decision-making, including profiling, and the inherent right to an explanation applies when a decision is made without any human involved. This decision must produce legal effects concerning the data subject or similarly significant effects.[87] A decision that has a similarly significant effect is something that has an equivalent impact on an individual's circumstances, behavior or choices.[88] Automated decisions made by an AI computer program, with a significant effect on peoples' health or right to treatment, may be subject to this provision. The provision also gives the data subject a right to an explanation on the reasoning behind the decision, which may be challenging for innovator using AI-technology as one not always know how the result was produced, often referred to as the black box problem.[89] To be truly transparent and in line with the basic principles of the GDPR, innovators should work on glass box AI and hence be able to give the data subject any explanations needed.[90][91]

The controller is obliged to erase personal data without undue delay when the purpose of the processing is achieved, if the data subject withdraws a consent, if the data subject objects to the processing in question and if the personal data have been processed unlawfully.

4.6 Obligations of the controller

In addition to the obligations explained above, several other obligations apply to the controller as requirements on data protection by design and to implement appropriate technical and organizational measures to ensure an adequate level of security considering the risk of the processing.[92] The controller must also conduct data protection impact assessments and enter into data processing agreements if a processor is used.

4.6.1 Data protection by design and by default

The obligation to ensure data protection by design and by default require that data protection is included from the start when designing new products and processes. The innovator must take this approach when creating new technologies, systems and processes which all controllers

[80] Note that there are other rights not mentioned in this report, cf. the GDPR III.
[81] This is in line with the purpose limitation in the GDPR article 5 (1) b).
[82] The GDPR articles 13 and 14.
[83] Ibid. article 12.
[84] Ibid. article 15.
[85] Ibid. article 20.
[86] WP 242.rev.01. Guidelines on the right to data portability, as last revised and adopted 5 April 2017, Article 29 Working Party.
[87] The GDPR article 22.
[88] Information Commissioner's office (ICO), Guidelines on automated decision-making: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-gdpr-say-about-automated-decision-making-and-profiling/#id3
[89] AI and Privacy, Datatilsynet (2018): https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf
[90] How Much Do You Know About Your Black Box?, Steve Roemerman (Forbes, 2019): https://www.forbes.com/sites/forbestechcouncil/2019/11/05/how-much-do-you-know-about-your-black-box/#239f924ee688
[91] Machine Learning in Medicine: Opening the New Data Protection Black Box, Feretti et al., European Data Protection Law Review, Volume 4, Issue 3 (2018).
[92] The GDPR articles 25 and 32.

processing personal data must comply with. The framework is based on proactively embedding privacy into all phases of the design and operation of IT systems, network infrastructure and business from the early design and code, through testing and deployment and through productive operation.[93] To fulfill this obligation, innovators must constantly throughout their innovation activities work with default settings in health apps which for example ensure that only the health data needed are processed, that erasure of data is automated or that pseudonymization is an integrated mechanism.

The GDPR also requires that the controller implements measures to ensure, by default, that the controller only process personal data which are necessary to achieve any purpose.[94]

4.6.2 Requirements on personal data security

The GDPR requires both the controller and the processor to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. Following an evaluation of the risk, consideration should be made to the nature, scope, context and purpose of the processing. Evaluation of the risk and the assessment of what is considered appropriate differ over time considering the rapid technological development, as well as the nature, scope, context and processing purpose. Pseudonymization can reduce risk but is not intended to preclude any other data protection measures.[95]

The highest possible standards for security and data protection are central to developing and exchanging electronic medical records.[96] It may be argued that the same considerations should be applied for secondary use of health data for development and innovation purposes.

It appears to be consensus on the need of interoperable data and platforms to enable both free and secure flow of health data.[97] As the requirements of information security will increase by the number of data subjects and the amount of health data per data subject it may be challenging to ensure an adequate level of data protection. This has been evident in different apps developed to battle COVID-19. The European Data protection Board has published guidelines on how to use location data and contact tracing tools in connection with the COVID-19 outbreak.[98]

4.6.3 Data protection impact assessment

An innovator should note that a Data Protection Impact Assessment (DPIA) is required when the processing could result in a high risk to the rights and freedoms of the data subjects. The DPIA shall be carried out *prior* to the processing and is an integral part of the 'data protection by design and by default'. A DPIA may be described as a process for building and demonstrating compliance. The DPIA process is designed to describe the processing, assess the necessity and proportionality and help manage the risks to the rights and freedoms of the data subjects as well as determine measures to address them.[99]

There are conditions to what a DPIA shall contain[100] and every national Data Protection Authority have issued a list of processing where a DPIA always will be required.[101] These lists should be checked as a part of every innovation activity including processing of personal data. Where the DPIA indicates that the processing would result in high risk for the data subject, the controller is obliged to consult with the data protection authority prior to the processing.[102]

4.6.4 The use of processors

When the controller uses a processor to process personal data, the controller is obliged to assess whether the processor will be able to uphold the requirements in the GDPR. The processing shall be governed by a data processing agreement, which must fulfill certain requirements.[103]

A pre-requisite when entering into a data processing agreement is that the processor processes personal data *on behalf* of the controller. Processing by a processor will typically happen when a controller outsources processing of personal data that the controller could do for themselves, for instance information technology (IT) services such as cloud services, PaaS, IT-support, maintenance and data storage but also when a controller hires a tech company to for instance develop an app if this includes processing of personal data.

---

[93] The 'privacy by design principles', seven in total, were first introduced by privacy authorities in Canada in the 1990's, cf. also the GDPR recital 78 and Opinion 5/2018 Preliminary Opinion on privacy by design page 13 (37).
[94] This is in line with the principle on data minimization.
[95] Recital 28, Intersoft Consulting: https://gdpr-info.eu/issues/encryption/ is currently considered 'state of the art' data protection officers usually rely on the definitions set out in information security standards like ISO/IEC 27001 or other national IT-security guidelines
[96] COMMISSION RECOMMENDATION of 6.2.2019 on a European Electronic Health Record exchange format p. 3 (12).
[97] Deloitte Insights, Digital health technology, Global case study of health care transformation, A report from the Deloitte Center on Health Solutions (2019)
[98] Guidelines 04/2020, European Data protection Board.
[99] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "*likely to result in a high risk*" for the purposes of Regulation 2016/679 (WP 248 rev.01), Article 29 Working Party.
[100] The GDPR article 35 (7).
[101] https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev.01) page 9 -13.
[102] The GDPR article 36.
[103] The GDPR article 28.

4.7 Transfer of and transborder access to personal data

The GDPR restricts the transfer of personal data out of the EU/EEA.[104] Countries outside EU/EEA are in this context referred to as 'third countries'. To ensure that the level of protection of the data subjects guaranteed by the GDPR is not undermined when transferring personal data to third countries or an international organization, such transfers shall only take place if certain conditions are complied with.

The European Free Trade Association (EFTA)[105] countries Iceland and Norway are not considered to be third countries as the countries have adopted the GDPR. The same applies for Åland.[106] Greenland and the Faroe Islands are both countries outside the EEA and not part of the EFTA countries. However, the EU-Commission has decided that the Faroe Islands provide an adequate level of protection.[107]

The transfer of personal data includes all disclosure of personal data, hereunder copy or transfer via a network, or through any other means Note that it is considered transfer of personal data if support personnel outside the EEA can access personal data stored within the EEA.[108] Innovators should be aware of this issue if considering cloud services and service providers offering support 24/365 as this is often provided from third countries.

There are different grounds of lawful transfer to third countries.[109] The European Commission may have decided that the third country ensures an adequate level of protection[110] or the controller or the processor may have provided other appropriate safeguards.[111]

As the GDPR covers all countries within the EU/EEA, those countries will provide an adequate level of data protection. The aim of the GDPR is also to ensure free flow of personal data within the internal market. Hence, transfer of personal data within this is not subject to any special conditions.

[104] The GDPR article 44.
[105] Liechtenstein is also member of EFTA.
[106] Cf. this report chapter 8.
[107] This adequate decision does not cover the authorities of the Kingdom of Denmark in the Faroe Islands, please refer to this report section 6.1 for further on the adequate level decision and the difference between the two Faroese acts regulating data protection.
[108] Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/
[109] The GDPR articles 44-46.
[110] The GDPR article 45 and https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[111] The GDPR article 46.

5. Denmark

5.1 Introduction

As health data constitutes a distinctive and special category of personal data, it is firmly regulated under Danish Law.

In Denmark, health data is interpreted in accordance with the definition of special categories of personal data in the GDPR, including the individual's contact with the health care sector.

Generally, health care personnel are subject to professional secrecy and must treat information on patients' health conditions with confidentiality. However, there are exemptions to the professional secrecy in both the health legislation and the data protection legislation, which provide legal basis for access to non-anonymized health data for secondary use.

Though, neither the Danish health legislation nor the data protection legislation refer to nor address access to health data for *innovation* purposes and, therefore, do not establish the required legal basis. Hence, access to non-anonymized health data for the purpose of innovation must be based on *consent* from each data subject.

Such consent must be specific and given in relation to a specified processing purpose and must further be informed, unambiguous and requires an affirmative action.

When legal basis exists the relevant health data may be applied for. The health data is primarily stored in medical records and in several different registries. In Denmark, no shared entrance to all health data exists. In certain cases, there are several steps in the application process and further, permits from authorities may be required.

As existing legislation does not provide legal basis for such shared entrance, nor access to health data for innovation purposes without obtaining consent, it is difficult for innovators to access non-anonymized health data in Denmark.

In terms of transborder access, health data can generally be transferred transborder on similar grounds as domestically. Greenland and the authorities of the Kingdom of Denmark in the Faroe Islands constitutes an exception in this regard, as they are not recognized as providing an adequate level of protection.

5.2 Danish health care system and information resources

The Danish health care system includes various public institutions and functions, hereunder the regions and municipalities. In addition, private operators contribute to the maintenance and development of the system.

Health data is collected by health care personnel and are stored in medical records. Most information from medical records are accessible electronically (e-journals) for health care personnel and patients at www.sundhed.dk. The platform further provides access to the Joint Medicine Card[112], which contains information on medicines, including prescriptions and delivered medicines. The Joint Medicine Card can also be accessed by patients using an app called "My Doctor"[113], where also further information about diagnosis, treatment plans, etc. is available. Note that different regions use different systems for electronic medical records (EPJ-systems), which may pose challenges for accessing health data.

There are also several registries and biobanks, both public and private, established for health data storage in Denmark.[114] Worth mentioning in this regard are the National Patient Registry, Regions' Bio- and Genome Bank, Statistics Denmark, The Regional Nationwide Clinical Quality Databases, Denmark's National Biobank and the National Genome Center. Each registry keeper has conducted guidelines for application procedures and approval of access to their respective registries and application for access to each registry must as a rule be filed with each of the registry keepers.

The Danish health care sector has high-quality information resources and well-established digitalized register practices. For example, the National Patient Registry contains data of all persons who have been in contact with public and private hospital services. The information resources contain extensive and complete nationwide data and a variation of different disease areas, and as a result of the civil registration system (ID-numbering), it is possible to link data between the different registries.

However, despite a well-established and comprehensive digital register system, health data is not centrally available under Danish Law.

Though, an overview of information resources within the Danish health care sector, including which variables are contained in each database, is provided at www.danishhealthdata.dk. This national data catalogue

[112] In Danish: Fælles Medicinkort.
[113] In Danish: Min Læge-app.
[114] Approximately 160 registers are established in Denmark.

also provides descriptions of how to apply for access from the different information resources.

Further, for access to health data for research purposes, Denmark has invested in a technical platform called the Researcher Machine, which enables access to health data from specific registries through applications to the Researcher Service at the Danish Health Data Authority. The platform enables access to health data necessary for the specific project from certain registries.[115]

Generally, access to Danish health data requires approval from relevant authorities. Worth mentioning are the Researcher Service, Statistics Denmark[116] and the Danish Regions. Access to the registries and biobanks may further depend on approval from the Danish DPA and the Danish Scientific Ethics Committee System[117] (or the Danish Patient Safety Authority[118]).[119]

5.3 Legal reforms enabling secondary use

In Denmark, several health strategies and legal reforms have addressed access to health data for secondary use purposes. These propositions have mainly addressed access to health data for research purposes, while access for innovation purposes only has been addressed to a limited extent.

In 2015, the Danish Regions presented a common regional policy to facilitate for research and innovation by making health data available for health research projects. The policy included public-private collaborations, i.e. collaborations between the state and universities for the establishment of homogeneous terms for use of health data for research and innovation. However, note that it was stated that only anonymized, pseudonymized or encrypted health data could be transferred to private operators.[120] The Danish Regions further wanted to examine the possibilities of establishing "researcher machines" which were thought to provide easier access to regional health data for researchers to benefit research and innovation.

Based on the aims of the 2015 policy, the Danish Committee of Health and Elderly[121] and the Danish Regions created a plan of action[122] with the purpose of realizing the policy's vision regarding use of health data. Through dialogue with the state, the Danish Regions wanted to discuss the need for a modernization of the legislation regarding use of health data.

In December 2016, the Ministry of Health and Elderly and the Danish Regions prepared a strategy called the 'National Strategy for Personalized Medicine 2017-2020'.[123] To benefit patients through new knowledge and treatment forms, it was stated that researchers must have secure, quick, and easy access to pseudonymized data. Further, to facilitate for research and innovation through collaboration on personalized medicine, it was stated that a more joint infrastructure for the collection and storage of biological material and data was required, and further that genomics research should be international and deeply integrated in the health care system.

In 2017, all parties of the Danish Parliament entered into an agreement on use of health data. The agreement included seven key principles on how health data, in a secure way, may be used for quality assurance, research on new treatment forms for the benefit of patients, etc.[124]

Further, in 2018, the Danish government issued the Amendment Act[125], partly concerning one of the primary initiatives of the National Strategy for Personalized Medicine 2017-2020; the establishment of the National Genome Center.

At the time of this report, the latest act[126] on this subject relocates the competence to approve scientific projects from the Danish Patient Safety Authority to the regional scientific ethics committees, for the purpose of more efficient access to information in medical records.

5.4 General principles on use of health data

Access to health data is strictly regulated and must comply with the GDPR's basic principles of processing[127] and requires legal basis.

Access to non-anonymized health data from medical records for secondary use generally requires either a written consent from the patient whose data is being

[115] For an overview of registries accessible through the Researcher Service: https://sundhedsdatastyrelsen.dk/da/forskerservice/for-du-soger/registre-og-dokumentation
[116] Similar to the Danish Health Data Authority's Researcher Machine, Statistics Denmark have their own search engine called "research machine" and a hereto related researcher service: http://www.dst.dk/extranet/forskningvariabellister/Oversigt%20over%20registre.html
[117] The Danish Scientific Ethics Committee System consists of the National Scientific Ethics Committee and the Regional Scientific Ethics Committees.
[118] As of 1 July 2020, the authorization to permit access to health data will be transferred from the Danish Patient Safety Authority to the regional councils.
[119] If a health scientific research project includes clinical trials involving medicines, the project may not only be approved in accordance to the above, but the Danish Medicines Agency must also be involved in the approval of the project.
[120] Sundhedsdata i spil, Danske regioner 2015/3.
[121] Appointed by the Danish Parliament and placed under the Ministry of Health and Elderly.
[122] Handleplan for bedre brug af sundhedsdata i regionerne, Danske Regioner (2015/3).
[123] Personlig Medicin til gavn for patienterne, National Strategi for Personlig Medicin 2017-2020, Sundheds- og ældreministeriet/Danske regioner (2017).
[124] Read more about the agreement: https://www.sum.dk/Aktuelt/Nyheder/Sundhedspolitik/2017/Februar/Bredpolitisk-aftale-om-principper-for-brugen-af-sundhedsdata.aspx
[125] The Danish Act no. 728 of 8 June 2018 on Amendment of the Danish Health Act (The Amendment Act).
[126] The Danish Act no. 1436 of 17 December 2019 on amendment of the Danish Committee Act, the Danish Health Act, the Danish Act on Complaints and Compensation regarding the Health care System and the Danish Act on Medicines.
[127] See this report chapter 4.

disclosed (the data subject) or a statutory exemption allowing access to health data for secondary use, typically combined with permits from one or more relevant authorities,[128] or as for access to health data from registries, etc. permits from one or more registry keepers. Hence, both statutory exemptions and consent provide legal basis for secondary use.

As for health data, statutory exemptions are mainly placed in the health legislation, in accordance to which health data, for example, may be accessed for the purpose of an approved health scientific research project.

If no statutory exemptions provide legal basis, the patients' consent must be obtained for access to health data. The consent must comply with the conditions laid down in the data protection legislation. Please refer to this report section 4.3.2 regarding the requirements for validation of a consent, as these requirements are applicable in Denmark. Though, the Danish Data Protection Act[129] prescribes a stricter age-limitation, after which anyone under 15 years of age are unable to consent to the processing of health data.[130] If the data subject is younger than 15 years old, the innovator must obtain a consent from the person who has the custody of the data subject.

Further, the consent must comply with the conditions laid down in the health legislation, which prescribes that the consent must be given at the time of the actual need for disclosure or when the information is retrieved and entered in the medical record. The consent must further be written, unless the character of the case or specific circumstances indicates otherwise, and it must be included in the medical record.[131] Finally, the consent lapses one year after it has been given.[132]

5.5 Legislation

5.5.1 General

The Danish Data Protection Act implements and supplements the GDPR (collectively the Danish Data Protection Legislation) and applies to all processing of personal data in both the public and private sector. Though, the Danish health legislation supplements and takes precedence over the Danish Data Protection Act.

5.5.2 Data Protection

According to the Danish Data Protection Legislation, processing of *personal data* must;

a) comply with the basic processing principles in the Danish Data Protection Legislation; and
b) be based on a legal basis either in the Danish Data Protection Legislation or any special legislation.133

These two requirements are considered cumulative.

Firstly, processing of personal data *must comply with basic processing principles, such as purpose specification* and *limitation*.[134] Generally, personal data must therefore be collected for specified, explicit and legitimate purposes, and cannot be further processed in a manner incompatible with these purposes.

If a specific purpose is stated in any applicable special legislation, the data can only be accessed or processed by the data controller for the stated purpose. If no purpose or legal basis are stated in the special legislation, the legality of a specific processing must be assessed in accordance with the Danish Data Protection Act.

Secondly, processing of personal data must be based on a legal basis. An explicit consent[135] from the data subject can constitute legal basis for processing and transfer of health data, also for other purposes than the data was originally collected for.[136]

Besides consent, applicable special legislation may constitute a legal basis for processing. For example, disclosure of data to a clinical quality database does not require a consent from the data subject.[137]

Specific regulation may apply to personal data considered as *health data*. According to the Danish Data Protection Act, the competent minister may lay down more detailed rules for use of health data[138], including genetic data.[139] The authorization may be used to introduce regulations for subsequent use of health data and genetic data for other purposes *compatible* with the original collection purpose.

Specific regulation further applies when the health data (i) relates to biological material[140], (ii) is processed outside the territorial scope of the GDPR (article 3) or (iii) is

[128] E.g. permission of a health scientific research project, unless disclosure is required e.g. by law or contract.
[129] The Danish Act no. 502 of 23 May 2018 on Data Protection (Danish Data Protection Act)
[130] Cf. the Executive Order Regarding Information and Consent section 8.
[131] In accordance with Executive Order no. 530 of 24 May 2018 on Authorized Health care Personnel´s Medical Records section 13 (1)-(2), the medical record must show, if the patient has expressed any restrictions on the disclosure of information.
[132] Cf. Executive Order no. 359 of 4 April 2019 section 10.1 regarding information and consent in connection with processing, disclosure and collecting of health data, etc. (Executive Order Regarding Information and Consent) section 10 (4).
[133] For example, the Danish Health Act.
[134] Cf. this report section 4.2.4.
[135] For specific requirements for consent, see this report section 4.3.2.
[136] A patient cannot give consent to the National Genome Center's processing of genetic information or information regarding health-related conditions for purposes outside of the scope of section 223b in the Danish Consolidation Act no. 903 of on 26 August 2019 on Health ("Danish Health Act") cf. associated bill no. 146 of 9 February 2018 regarding amendment of the Danish Health Act.
[137] Cf. the Danish Health Act section 196 (4) and this report section 4.2.6.2.
[138] The GDPR article 9 (1).
[139] The Danish Data Protection Act section 5 (3)
[140] Approval from the Danish DPA is not required for transfer of personal data, generated from biological material cf. the Danish Data Protection Act section 10 (3).

requested for publication in a recognized scientific journal or similar. In these situations, disclosure of health data requires prior authorization from the supervisory authority.[141]

5.5.3 Professional secrecy

Pursuant to the Danish Health Act, health care personnel are subject to professional secrecy. This means that in the conduct of their profession, health care personnel must consider the confidentiality of their experiences or presumptions regarding a person's health condition and/or other confidential information. Thus, processing of health data obtained in the conduct of health care personnel's profession, including activities covered by other health legislation, will be subject to the professional secrecy.

Under Danish Law, there are several exemptions from the professional secrecy. Some exemptions are based on the consent of the patient concerned, while other are based on alternative legal basis. However, no Danish act provides innovators an alternative legal basis for access to health data[142], thus the concerned patients' consent must be obtained for the purpose of innovation.

5.5.4 General regulation on health research

The Danish Health Act

Access to health data from medical records for research purposes is regulated by the Danish Health Act.[143] Accessible data in this regard are health data, additional sheer private matters and other confidential information.

Without the patients' consent, data may only be transferred to a researcher for the purpose of an approved health scientific research project[144] or for statistics or planning purposes after prior approval. The term *researcher* includes researchers with a medical or other educational background.

The act does not provide legal basis for transfer of data from medical records for the purpose of a *pure innovation project.*[145] Therefore, the patients' consent is required for access to data for these projects.

The Danish Committee Act

The Danish Committee Act[146] regulates approval of health scientific research projects and access to non-anonymized health data including biological material for such projects[147]. For access to such data without the patients' consent, it is decisive that the project is in fact considered a health scientific research project.

A health scientific research project involves trials on live-born human individuals, including testing of medicine or clinical testing of medical equipment. The term *health scientific* is understood as treatment, examination, prevention and rehabilitation, while *research* is understood as a planned business with the purpose of systematically obtaining knowledge about diseases' occurrence and regarding prevention, diagnostics and treatment hereof.[148] Hence, a health scientific research project is characterized as an activity planned after a *scientific method*, which aims at producing new valuable knowledge about human's biological and physiological processes. Danish law does not further emphasize the borderline between research and innovation.

As a rule, all health scientific research projects are subject to a duty of notification and must be registered in the scientific ethics system.[149][150] For approval of the health scientific research project, the purpose of the project must be to generate new knowledge other than treating the patient. Moreover, it is a condition for approval of a project that the Data Protection Legislation is complied with.[151] If access is not permitted by a scientific ethics committee, the patients' consent is required to gain access to health data.[152] Please note that projects only requiring anonymized human biological material are not subject to the duty of notifications.[153]

If a health scientific research project includes clinical trials involving medicines, the project may not only be approved in accordance to the above, but the Danish Medicines Agency must also be involved in the approval of the project. Inclusion of trial participants in clinical research always requires consent, the only exception being research on acute experimental situations involving trials without medicine testing. Consent to participation can always be withdrawn.

---

[141] The Danish DPA may lay down rules for the disclosure of data covered by the Danish Data Protection Act section 10 (1) and 10 (2), cf. section 10 (3) and Executive Order on Transfer of Personal Data Covered by the Danish Data Protection Act, section 10(1) and (2).
[142] Provided that the innovation project cannot be characterized as a research project.
[143] The Danish Health Act section 46.
[144] The Danish Consolidation Act no. 1083 of 15 September 2017 on Scientific Ethical Conducting of Health Scientific Research Projects (the Danish Committee Act), defines such projects.
[145] Provided that the project is not covered by any other exemptions laid down in the Danish Health Act.
[146] The Danish Committee Act implements directive 2001/20/EF and the EU Council's convention on human rights and biomedicines.
[147] Research projects which is not subject to this act, but of significant societal importance, must be approved by the Danish Patient Safety Authority.
[148] Research differs from quality development projects and quality control, which are activities included in the operation of the hospital service (on a local level).
[149] The Danish Committee Act section 14 (1). For exemptions to the duty of notification cf. section 14 (2)-(5).
[150] Cf. Guidelines no. 9154 of 5 May 2011 on Notification of a Biomedical Research Project to the Scientific Ethics Committee System (Guidelines on Biomedical Research Projects).
[151] Cf. the Danish Committee Act section 20.
[152] Cf. the Danish Health Act section 46 conversely.
[153] Unless the project is subject to the Danish Act no. 902 of 23 August 2918 section 25 on Assisted Reproduction in Connection with Treatment, Diagnostic and Research etc.

5.6 Access to health data for secondary use

5.6.1 Access to health data in medical Records

General

Public and private health care providers must keep manual or electronic medical records.[154] A medical record must be kept for each patient and the record must contain information necessary for providing a good and secure patient treatment. Information included must be readable and cannot be deleted. Information from a medical record must be stored for ten years as of the latest amendment in the medical record.

Medical records are mainly stored electronically. The Danish regions uses different electronic medical record-systems (EPJ-systems), which are not collaborative. Although the platform www.sundhed.dk provides access to e-journals, the Joint Medicine Card, etc., certain EPJ-systems are not compatible for transfer of all collected health data to e-journals. Thus, health care personnel from different regions do not always have access to all collected health data on the concerned patient. These challenges may hinder access to health data for both primary and secondary use purposes.

Health data in medical records are generally subject to professional secrecy, which means that access is dependent on either the patients' consent or an alternative legal basis.

The patient's consent and access to own medical records

Upon request, patients have a right to access own medical records composed by health care personnel and kept at public and private hospitals, clinics etc. Patients also have a right to receive information of manually processed data, hereunder the processing purpose, who the recipients of the data are, and information regarding the origin of the data.[155][156]

Access to medical records may be given electronically, by review of the medical records at the place of treatment, or by transcript or copy to the patients. The type of access is dependent on the patient's request.

Patients may also access own health data, including course of treatment, medicine, lab results, registered by the public health care sector at the e-journal, the Joint Medicine Card, at www.sundhed.dk.

Access to health data in medical records for health scientific research projects

Health data, additional sheer private matters and other confidential information from medical records can without the patient's content be disclosed to a researcher for scientific purposes on prevailing terms.[157] Firstly, such data can be disclosed without the patient's consent if the project is characterized as a health scientific research project permitted in accordance with the Danish Committee Act. Please refer to this report section 5.5.4 on the Danish Committee Act for details on what is required for a project to be characterized as a health scientific research project.

> *Innovators cannot get access to health data from medical records without the patients' consent.*

Secondly, such data can be disclosed without the patient's consent in connection to a specific research project permitted by the Danish Patient Safety Authority. The Danish Patient Safety Authority will determine whether the project is of significant social interest as well as the terms of the disclosure.[158]

Please note that the authorized[159] health care personnel are responsible for collecting the disclosed information. Thus, researchers are not allowed to electronically collect information for medical records themselves. Subsequent inquiries to the individuals in question may only occur to the extent permitted by the responsible health care personnel who have treated the concerned individual. For example, the treating health care personnel may permit inquiries from researchers who use information from medical records to find qualified participants to a clinical research study or survey.

Thirdly, such data can be disclosed without the patient's consent for the use of statistic or planning purposes when permitted by the Danish Patient Safety Authority. This permission is not required when disclosure of the data is required by law.

Data collected for the use of scientific, statistics or planning purposes, may not later be processed for other purposes.[160] Publication of the collected information may only happen in a way where the data cannot be ascribed to private individuals.

---

[154] The Danish Consolidation Act no. 731 of 8 July 2019 on Authorization (the Danish Authorization Act) chapter 6.
[155] The Danish Health Act section 37 (1).
[156] In specific cases, patients have a right to refuse others from accessing their medical records.
[157] The Danish Health Act section 46 (1). Projects outside the scope of the Danish Committee Act, are permitted by the Danish Patient Safety Authority in accordance with section 46 (2).
[158] As of 1 July 2020, 'specific health data scientific research projects' will also be included in the Danish Health Act section 46, cf. the Danish Act on amendment of the Danish Committee Act, the Danish Health Act section 2 (3).
[159] Meaning 'authorized' as characterized in the Danish Authorization Act.
[160] The Minister of Health and Elderly may lay down detailed rules on disclosure and processing of such data for other purposes, if necessary for the protection of the data subject's vital interests, cf. the Danish Health Act section 48 and the Danish Data Protection Act section 10 (5).

Access to health data in medical Records for quality development and quality assurance

Authorized health care personnel can with the patient's consent look up electronic medical records and other systems that supplement the medical records, for the aim of collecting information about the patient's health conditions and other confidential information for other purposes than treatment.[161] The collection of such information must be considered impartial and necessary.

Information from electronic medical records and other systems may also be collected *without the patient's consent* if performed by authorized health care personnel and:

a) the collection is necessary for quality assurance or quality development of the course of treatment;
b) the processing of information is considered of significant societal importance and occurs for statistical purposes considering the patient's integrity and private life;
c) the management of the place of treatment has given permission to collecting based on concrete criteria for the authorized health care personnel;
d) the information in question is registered in the electronic systems at the relevant place of treatment less than five years prior to the collection; and
e) it subsequently is possible to identify that the collection has occurred for quality assurance or quality development.

Quality development is understood as information in medical records that is used to systematically improve the quality of treatment. It can be used to examine work procedures and processes, and may concern e.g. effective treatment, security for the patient and cost-effectiveness.[162]

Personal data collected for statistical studies can only be processed for this purpose. Study results can be used for general assurance and development of quality at the place of treatment or e.g. on a regional level, if the data is aggregated and non-personally identifiable.

> *Consent is as a rule needed for access to health data for other purposes than treatment. However, access to health data for the purpose of quality assurance and quality development is an exception hereto.*

Please note that the patient can refuse to the collection of information without their consent. Such refusal may be given orally or in writing to the responsible health care personnel at the place of treatment and shall be included in the medical records.

The above only includes quality work which is performed by a region, municipality or a private place of treatment[163] and does not include researchers as such. Though, researchers who are also authorized health care personnel may collect the data with the patients' consent for the purpose of e.g. surveillance of the operation on a local level. It is a prerequisite that the researcher is only provided with a technical access to the health data needed for the specific project.

For the purpose of extracting more generalizable knowledge that extend beyond surveillance of the operation on a local level, both researchers who are and are not authorized health care personnel must use other legal basis provided by the health legislation to get access to the information.[164] Otherwise, the patient's consent must be obtained. The same applies for innovators.

Access to health data in medical records for other Purposes

With the patient's consent, health care personnel can disclose information regarding the patient's health and other confidential information to other health care personnel, authorities, organizations, private individuals and others for non-treatment purposes.

Information can also be disclosed *without the patient's consent* when disclosure is[165];

1. required by law and the information is considered essential for the case handling of the receiving authority;
2. necessary to protect public interests, the patient, health care personnel or others;
3. necessary for an authority to perform supervisory and control responsibilities;
4. to an accreditation body approved by the government, and the information is considered necessary to document specific accreditation procedures; or
5. required to follow up any accidental incident in the region, municipality or a private hospital.

It is the health care personnel in possession of the confidential information who determines whether disclosure is justified in the specific case.

[161] The Danish Health Act section 42d (1).
[162] Quality assurance and quality development projects only can be performed in accordance with the Danish Health Act section 42d (2), not section 46.
[163] Understood as authorized health care personnel who are preparing a scientific project, etc.
[164] Consent must be obtained for collecting, see the Danish Health Act section 43 or 46.
[165] Ibid, section 4 (2).

If information is manually disclosed in accordance with one of the conditions above, the party concerned shall be informed of the disclosure and its purpose as soon as possible. An exception is made for information that can be omitted under other legislation or for reasons of public or private interests, correspondent to those protected by this legislation. Such disclosure is not subject to the GDPR, as the GDPR applies to processing of personal data within the meaning of wholly or partly automatic or other non-automatic processing of personal data, which is or will be kept in a register.[166] If information is disclosed within the scope of the GDPR, the data controller (region, general practitioner and/or others) must notify the party concerned.

For disclosure of such information for innovation purposes, no exceptions apply. Thus, disclosure of data to innovators requires the patients' consent.

> *Private companies and innovators cannot access non-anonymized data from the National Prescription Register.*

5.6.2 Access to health data in national health registries

General

Denmark has several national health registries containing data relating to the health of the Danish population and/or services of the health care sector. Denmark also has a unique system of ID-numbering of the Danish citizens (the Civil Registration System), which provides opportunities for linking data from various registries.

The responsibility of the registries is placed with registry keepers, who operate as data controllers for the underlying registries. The six major registries or data entrances are the Regions' Bio- and Genome Bank, the Researcher Machine at the Danish Health Data Authority, the Research Machine at Statistics Denmark, the Regional Nationwide Clinical Quality Databases, Denmark's National Biobank and the National Genome Center.

The registries contain different health data. Application for access to health data from a register can be submitted to the registry keeper concerned. Each registry keeper has conducted guidelines for application procedures and approval hereof. Access to the requested data may further require that necessary approvals are obtained, for example from the Danish Data Protection Agency (the Danish DPA) or a scientific ethics committee.

Access to data from prescription registers

Pharmacists are subject to professional secrecy and cannot unfoundedly disclose or exploit confidential information[167] collected in connection with their businesses.[168] Certain exceptions apply, e.g. if disclosure is necessary based on legitimate public interests.

The National Prescription Administration Register contains information regarding prescription of medicines, including identifiable information[169] of the issuer of the prescription. Such information can be disclosed to the prescription issuer, the patient and administrative authorities within the health care sector for statistical or scientific purposes of significant public importance.[170] Hence, disclosure of non-anonymized data from the register *to private businesses and innovators is not permitted*.

Another prescription register is the National Prescription Register, which contains information regarding prescription of medicines, including identifiable information of the issuer of the prescription and the patient. Such information may be disclosed to an exhaustive group of individuals consisting of personnel in the public health care administration, researchers employed by universities, patient associations, or Statistics Denmark,[171] for the use of statistical and scientific studies of significant public importance.[172] Hence, disclosure of non-anonymized data from this register *to private businesses and innovators is not permitted*.

Thus, the identifiable information cannot be disclosed to all parties involved, when projects are led by both public (as listed above) and private participants, for example innovators.

Disclosure from the registers must be necessary for the execution of the studies.

> *Public and administration authorities can get access to health data from the National Prescription Administration Register.*

[166] The GDPR article 2 (1).
[167] Confidential according to law or other provisions, or information required to be kept secret for significant public and private interests, cf. the Danish Act no. 801 of 12 June 2018 on pharmaceutical (Danish Pharmaceutical Act) section 3a (2).
[168] The Danish Pharmaceutical Act section 3a (1).
[169] Identifiable information is understood as non-anonymized data.
[170] Executive Order no. 1616 of 18 December 2018 regarding disclosure of information from the Danish Health Data Authority's National Prescription Administration Registry; the Danish Pharmaceutical Act section 11 (4) and Guidelines no. 9364 of 24 May 2018 regarding disclosure of information from the Danish Health Data Authority's National Prescription Administration Register and the Danish National Prescription Register (Guidelines on Information from Prescription Registers).
[171] The researcher must request access to the data at Statistics Denmark through the Researcher Service, cf. this report section 5.6.2.
[172] Executive Order no. 900 of 29 June 2017 regarding disclosure of information from the Danish Health Data Authority's National Prescription Register (Executive Order Regarding National Prescription Register), and Guidelines on Information from Prescription Registers.

The identifiable information accessible for an individual within the exhaustive group cannot later be further disclosed by the individual, neither to other researchers.[173]

Access to other health registries

As mentioned above, application for access to health data stored in the health registries must be submitted to the relevant registry keeper. For example, researchers can apply the Researcher Service[174] within the Danish Health Data Authority, for access to data in the Researcher Machine, which contains data from several different registers.

Prior to an application, any necessary permits must be collected. For example, health scientific research projects must be filed with a scientific ethics committee for approval,[175] and if data from both registers as well as from medical records are requested for a register research project, which does not include biological material, prior approval from the Danish Patient Safety Authority must be obtained.[176] For projects using only numbers and statistics (excluding non-anonymized data), no prior approval is required.

Surveys and interviews must be filed with a scientific ethics committee for approval if human biological material is included.[177] Surveys and interviews involving individual health related questions to individuals shall not be filed and approved by a scientific ethics committee if the answers are anonymous.

Prior to an application, researchers must also have created an overview of what data is necessary for the project. Documentation of relevant permits or approvals and a list of necessary information must be enclosed the application. This also applies for surveys and interviews.

Access to data from Statistics Denmark

Statistics Denmark operates with a similar system as the Researcher Machine at the Danish Health Data Authority, called the 'Research Machine', which contains microdata. In addition, Statistics Denmark has so called 'open data' at the statistics bank at www.statistikbanken.dk and www.dst.dk, meaning that the information is publicly available. Information stored herein can be accessed instantly and used for commercial as well as non-commercial purposes.[178] This is opposed to the Researcher Machine, which provides access to contained data to researchers only.[179]

Further, Statistics Denmark prepares customized statistics upon payment. In these circumstances, non-anonymized data of individuals is not included.[180]

5.6.3 Access to health data in clinical quality databases

Authorized health care personnel, private individuals, and institutions operating hospitals are required to provide central health care authorities with information of their activities.[181] Hereunder, health care personnel are required to report, among others, relevant information regarding patient's health conditions and other confidential information contained in medical records to clinical quality databases.[182]

To access the clinical quality databases, an application for access must be submitted to the Researcher Service within the Danish Health Data Authority. The application procedure corresponds to the application procedure for access to data in the national health registries.

The Danish Health Data Authority must enquire the data controller authority of the database in question, for the purpose of supporting correct use and interpretation of the received data prior to transfer of data originating in the databases.[183][184]

> *Access to health data stored in approved clinical quality databases for the purpose of a specific research project is possible without the patients' consent.*

5.6.4 Access to health data in biobanks

General

In Denmark, biobanks are characterized as either research biobanks or clinical biobanks. A research biobank is

[173] Disclosure of information that has been processed for scientific and statistical purposes to a third party, requires approval from the Danish DPA if the disclosure relates to biological material, occurs for processing outside the GDPR's territorial scope, or for publication in a recognized scientific journal, cf. the Danish Data Protection Act section 10 (3) and Guidelines on Information from Prescription Registers.
[174] The Researcher Service counsels on the use of register data kept in the Researcher Machine and permits access hereto provided that the application fulfills the requirements.
[175] The Danish Committee Act section 14 (2).
[176] The Danish Health Act section 46 (2).
[177] The Danish Committee Act section 14 (2).
[178] Read more about open data here: https://www.dst.dk/da/OmDS/omweb
[179] Access to data for researcher: https://www.dst.dk/da/TilSalg/Forskningsservice/Dataadgang
[180] Access to statistics upon payment: https://www.dst.dk/da/TilSalg
[181] The Danish Health Act, section 195 (1).
[182] The Executive Order no. 585 of 28 May 2018 on reporting to approved clinical quality databases and disclosure to the Danish Health Data Authority (Executive Order on Clinical Quality Databases), section 2 (2). For a list of existing clinical quality databases: https://www.rkkp.dk/om-rkkp/de-kliniske-kvalitetsdatabaser/ and for guidelines on application procedure, etc.: https://www.rkkp.dk/siteassets/forskning/retningslinjer_forskning_version5_1.pdf
[183] The Danish Health Data Authority receives information from the databases once a year, cf. the Executive Order on Clinical Quality Databases section 3 (1). The Danish Health Data Authority pseudonymizes the data immediately after the information is received.
[184] The Executive Order on Clinical Quality Databases section 3 (5).

established when biological material is extracted and stored in connection to a health scientific research project. In this regard, it is a prerequisite that the biological material is included as an integrated part of a health scientific research project.[185] A clinical biobank is established in connection to a person's contact with the health care sector and is used for clinical purposes, such as for prevention, diagnosis, treatment, etc. All biobanks are regulated by the Danish Data Protection Act and the health legislation.

In accordance with the Danish Data Protection Act, 'biobanks' are interpreted as manual registers and are subject to the provisions in the act.[186] Establishment of a biobank must be filed with the Danish Data Protection Agency, who will provide either a statement (public data controller) or a permit (private data controller) stating the terms for establishment.

The National Biobank provides researchers based domestically and abroad online access to aggregated data.

When biological material from a biobank is used for a health scientific research project, the Danish Committee Act applies. This implies that prior approval from a scientific ethics committee generally is required to access the material. Such approval is also required for projects using imported biological material when the research activities are performed in Denmark. However, such approval is not required for projects using only anonymous biological material.[187]

Biological material that a patient has submitted in connection with treatment can be transferred to *researchers* for use in an approved health scientific research project without the patient's consent unless the patient has decided[188] that its biological material shall not be used for other than treatment purposes.[189] The same applies for genetic information originating from biological material collected from treatment and stored in the National Genome Center.[190]

Material from the Regions' Bio- and Genome Bank can be disclosed for diagnostic purposes when an application is submitted by *a private or public researcher* that are responsible for the project which the material is requested for.[191] Hence, innovators cannot apply for the material in the Regions' Bio- and Genome Bank.

Access to health data and biological material from Denmark's national biobank

Denmark's National Biobank provides researchers online access to *aggregated data* submitted by all contributing biobanks.[192] Access is provided to both domestic and foreign researchers and enables researchers to create an overview of biological material accessible for various health research in Denmark.

Researchers can also be given access to *biological material* from Denmark's National Biobank after submission of a permit. Before submitting a request for biological material, the health scientific research project must have been approved by a scientific ethics committee. Then, the researcher can request the material through the Researcher Service at the Danish Health Data Authority after which the request will be delivered to Denmark's National Biobank's Nomination Committee who will decide on access.[193]

The National Biobank does not provide innovators access to biological material for innovation projects.

Access to health data for health scientific research projects with clinical trials

A health scientific research project with clinical trials includes any trials on humans with the purpose of identifying or testing clinical effects of trial medicines or identifying side effects for assessing the safety or effect of the medicines.

Health scientific research projects concerning clinical trials with medicines, which are covered by the Danish Medicines Act,[194] requires approval of the project by the Danish Medicines Agency.[195]

Researchers can get access to biological material for the purpose of an approved health scientific research project without the patients' consent.

[185] Guidelines on Biomedical Research Projects.
[186] Guidelines no. 83 of 22 September 2004 regarding Biobanks within the Health care sector.
[187] The Danish Committee Act section 14 (3).
[188] The Danish Health Act section 32 (1). Such decision is registered in the Register regarding Use of Tissue, cf. Executive Order no. 361 of 4 April 2019 Regarding the Register Regarding Use of Tissue.
[189] The Danish Health Act section 29 (4).
[190] The conditions in the Danish Health Act section 46 (1)-(2) must be met.
[191] The private researcher can only get access to data where identifiable information is removed, cf. the Danish Regions' instructions of 1 April 2016 regarding collaboration between the Regions' Bio- and Genome Bank and companies. Application for approval must be filed to the secretariat of the Regions' Bio- and Genome Bank.
[192] Contributing biobanks are e.g. biobanks established by hospitals, universities and other scientific research institutions.
[193] More on access: https://www.nationalbiobank.dk/adgang
[194] Danish Consolidation Act no. 99 of 16 January 2018 on Medicines (the Danish Medicines Act).
[195] Cf. the Danish Committee Act section 21 (1).

Health scientific research projects involving clinical trials require the participants' consent in general.[196][197] However, it is possible to apply for a dispensation from the required consent if the project is not considered to involve risk or in any other way be at strain for the trial participant.[198]

Consent from the trial participant provides the sponsor[199] or the sponsor's representatives, *direct* access to information in medical records, including electronic records, for the purpose of evaluating trial participants' health conditions which are necessary for the completion of the project.[200]

The consent to participate in such project can always be withdrawn. A withdrawal does not affect already processed data included in the project.

> *For health scientific research projects including trials on humans, consent from the trial participants must in general be obtained.*

5.6.5 Access to health data in public archives

General

All governmental authorities and institutions under the Danish state are required to submit their archives to the Danish Public Records.[201] The Danish regions and municipalities can choose to submit their archives to the Danish Public Records or keep them in their own archives.[202] However, archives subject to the Data Protection Legislation must be submitted to a public archive.[203]

Public archives containing information about individuals' private conditions, including health data, are accessible 75 years after submission.[204] If decided by the submitting authority, the information may be accessed earlier. In this regard, a statement from the Danish DPA is required.[205]

Anyone may apply for access to information not publicly accessible[206], in which the purpose for access must be enclosed the application. Approval is granted either by the keeper of public archives (e.g. the Danish Public Records) or by the municipality or regional council (for municipally or regional archives). When the requested archive unit includes personal information and former processing of the information has been subject to the Danish Data Protection Legislation, approval requires acceptance from the Danish Data Protection Agency.[207]

If access is granted, the applicant may not unjustified publish, transfer or exploit any information characterized as confidential by law or equivalent, for example health data. Copies of non-public information are permitted. However, such copies cannot be transferred without specific permission.[208]

Access to data from the Danish National Archives

The Danish National Archives has Denmark's largest collection of survey-based research data. The archive is accessible for researchers and students, who may request specific data, perform analysis online, and/or obtain access to register data and international survey data for research project purposes.[209]

If the requested data includes personal data, the Danish Data Protection Agency's prior approval is required. However, for anonymized data, no such approval is required. The Danish National Archives has a similar research service as mentioned above, available for researchers and students, as well as a joint search database, which includes several public archive collections accessible for private individuals for other than research purposes. Thus, innovators may also request and access data from this database.[210]

> *Archive units that contain health data are accessible upon 75 years of age. However, such units are accessible earlier with the Danish Data Protection Agency's permission.*

[196] Exception is made for acute experimental situations, which does not involve testing of medicines.
[197] The consent must be given freely, explicit and in writing. For further requirements for the consent, see Guidelines no. 161 of 12 October 2000 on Information and Consent in Connection with Involvement of Trial Subjects in Biomedical Research Projects and on Notification and Assessment of Research Projects in the Scientific Ethics Committee System.
[198] Cf. the Danish Committee Act section 10.
[199] A physical or legal person responsible for starting, management or financing of a health scientific research project.
[200] Cf. the Danish Committee Act section 3 (3) and the Danish Medicines Act section 89 (3).
[201] Cf. the Danish Archive Act section 12.
[202] Ibid. section 19 (1)-(2).
[203] An exception is made for information in the Danish General Medical Database regarding individuals' health data, if approval for collecting the information is not obtained, cf. the Danish Archive Act section 21a.
[204] The Danish Archive Act, section 23 (1).
[205] Ibid. section 23 (2).
[206] Meaning before the archives are 75 years of age.
[207] The Danish Archive Act section 34. The Danish DPA must ensure that the Danish Data Protection Act section 10 is not bypassed by disclosure of the information. The archive keepers may in connection with an approval lay down further rules for use of non-public accessible archives, cf. the Danish Archive Act section 41.
[208] The Executive Order on Public Archives section 18.
[209] More on access: https://www.sa.dk/da/forskning-rigsarkivet/benyt-surveydata/
[210] The data can be applied for here: https://www.sa.dk/find/

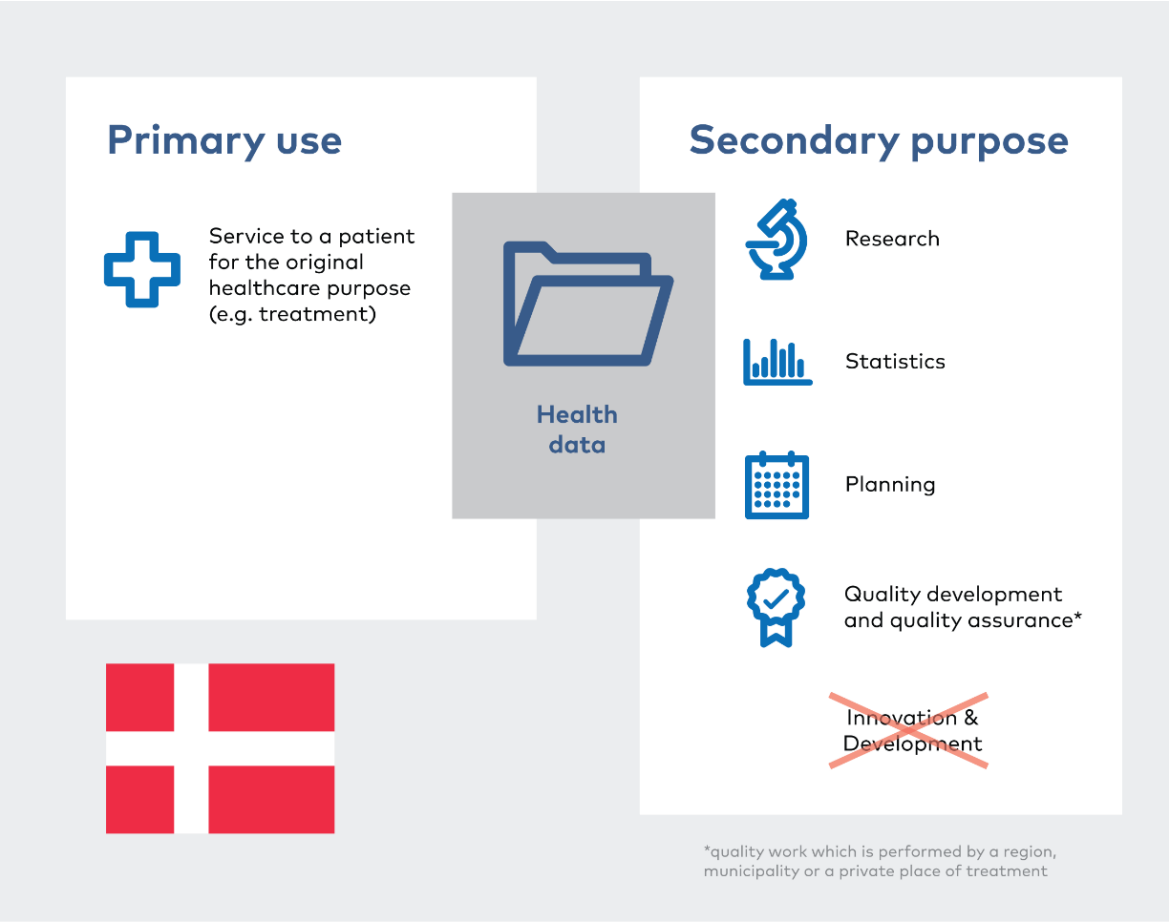


Figure 3 - Regulated division of primary and secondary use of health data in Denmark

5.7 Transfer of and transborder access to health data

5.7.1 General principles in the Danish Data Protection Legislation

Health data can be transferred to other countries and organizations within the EU and EEA, as well as to other countries and organizations considered to be secure third countries in terms of data protection, without meeting any additional requirements. An exception is made for actual transfer of biological material, in which prior approval from the Danish DPA must be obtained.[211]

Greenland is not considered to be a secure third country, thus transborder access to health data entails meeting further requirements. The same applies for transfer to the authorities of the Kingdom of Denmark in the Faroe Islands, since they are not recognized as providing an adequate level of protection. If none of the additional requirements for transfer are present, the transfer of health data is dependent on consent from the data subject.[212]

For transfer of health data for the sole purpose of carrying out statistical or scientific studies of significant societal importance outside the territorial scope of the GDPR, approval from the Danish DPA is required. This applies for transfers to Greenland and the authorities of the Kingdom of Denmark in the Faroe Islands.

Further, in special cases, the Danish DPA may prohibit, restrict, or suspend transfer of health data to non-secure third countries or international organizations.

5.7.2 Special regulation regarding transfer of health data

Generally, health data may be transferred to other countries or self governing territories in the Nordic region

[211] The Danish Data Protection Act cf. section 10.3(2).

[212] Public authorities cannot use consent as legal basis for transfer of health data to third countries.

if the requirements in the Danish Data Protection Legislation and health legislation are met.

However, the Danish Health Data Authority are prohibited from disclosing information from the Danish National Prescription Registry to foreign countries.

In lack of statutory provisions, consent from the data subject, as well as necessary authorization from authorities, may constitute legal basis for transfer of non-anonymized health data.

5.8 National obstacles

5.8.1 Permission from authorities

Permission from relevant authorities are generally required for access to health data for research purposes. Relevant authorities are typically a scientific ethics committee or the Danish Patient Safety Authority and, for projects involving testing of medicines, the Danish Medicines Agency. In addition, a permit from the Danish DPA may be required.

5.8.2 Lack of innovation specific regulation

Further, access to health data for the *purpose of innovation* is limited by law. A prerequisite for permission for access is that the project in question can be characterized as a research project in accordance with the Danish Committee Act. If the project is considered innovative, permission is denied. It poses challenges that the borderline between research and innovation is not further regulated or defined in the legislation, thus the authorities, primarily the scientific ethics committees are given a certain level of freedom to determine whether a project is considered to be research or innovation.

5.8.3 Decentralized registries

When legal basis, including necessary permission from the relevant authorities, is obtained, the researcher can apply for the non-anonymized health data.

The health data is primarily stored in different registries which contain different health data. The registries are managed by different registry keepers, thus there is no shared entrance to all available health data.

Although the national data catalogue provides easier search across the registers, and Denmark has several research machines, which enables access to health data from different registers simultaneously, there are no search engines including all available registers. Lack of such search engine or shared entrance complicates the process of identifying and collecting all available health data necessary for the specific project.

Further, collection of health data from specific registers also introduces certain challenges. The health data in the various registers are generally divided in accordance with the data source rather than content. Therefore, to identify and assemble relevant information for the specific project may be a complicated procedure.

Further, despite the existence of the national data catalogue, which provides an overview of all information resources, there is a risk that not all relevant data is being collected. Data may be stored in various registries or in minor registries not publicly searchable.

Two possible solutions to these obstacles are the establishment of a central entrance to all data, or data sandboxes.

6. The Faroe Islands

6.1 Introduction

Faroese law strictly regulates access to and transfer of health data, since this type of data constitutes a particularly sensitive category of personal data.

Generally, health care personnel are subject to professional secrecy and must treat information on patients' health conditions with confidentiality. However, there are exemptions to the professional secrecy in both the health legislation and the data protection legislation, which provide legal basis for access to non-anonymized health data for secondary use. As no such legal basis is provided for *innovation* purposes explicitly, access to non-anonymized health data for the purpose of innovation must as a rule be based on *consent* from each data subject if not covered by an exemption for any other secondary purpose.

As in Denmark, no shared entrance to all health data exists in the Faroe Islands, neither does a national data catalogue of available health data. As existing legislation does not provide legal basis for such shared entrance, nor access to health data for innovation purposes without obtaining consent, it is difficult for innovators to access health data in the Faroe Islands.

In terms of transborder access, health data can generally be transferred transborder without meeting further requirements. Although, in some cases notification to the Faroese Data Protection Agency (the Faroese DPA) is required. Transfer to Greenland is however subject to further requirements. This will in some cases also apply for transfer to Åland.

6.2 Faroese health care system and information resources

Except for the field of apothecary, health care is a joint responsibility between the Danish state and the Faroe Islands' Home Rule Government. The Danish Health Authority is the supreme authority, and the Danish Patient Safety Authority is the supreme health care professional supervisory authority.

The Faroese Home Rule Government is responsible for provisions concerning specific tasks, benefits and administration of the health services. The Faroese Minister of Health is responsible for health research matters, councils, committees, institutions and regulations within the health care sector.

As in Denmark, health data is recorded by health care personnel when providing health care. In addition to medical records, health data is stored in various registers and the Genetic Biobank.[213]

The Faroe Islands has limited information resources within the health care sector, presumably due to the limited size of their institutions. For example, the Statistics Faroe Islands must prioritize and only produce the most urgent and socially useful statistical data, which health data in specific is not considered to be.[214]

As in Denmark, there is no central entrance to all stored health data. Access is dependent on the type of data, what type of register/biobank the data is stored in, and who the registry keeper is.

Generally, access to Faroese health data requires approval from relevant authorities. Worth mentioning are the Genetic Biobank, the Gene Collection and Statistics Faroe Islands. Access to specific registers and the Genetic Biobank may also depend on approval from the Danish DPA, the Faroese DPA and the Faroese Scientific Ethics Committee System[215] (or the Danish Patient Safety Authority). Access to medical records may further depend on the approval of the Danish Health Data Authority.

6.3 Legal reforms enabling secondary use

In the Faroe Islands, health strategies and legal reforms regarding secondary use of health data have addressed access for research purposes, not innovation purposes specifically.

The Act on Human Genetics Research was introduced in 2005 to establish the necessary parameters for research into human genetics and encourage such research.[216] In this regard the Genetic Biobank was established in 2006 and developed an infrastructure for establishing and maintaining an active biobank for research purposes.[217] In recent years, the National Hospital of the Faroe Islands has been involved in several research projects in collaboration with the Genetic Biobank.[218]

[213] Cf. this report section 6.6.4.
[214] Statistics Faroe Islands: https://hagstova.fo/en/about-us
[215] The Faroese Scientific Ethics Committee System consists of the Faroese National Scientific Ethics Committee and the Faroese Scientific Ethics Committee.
[216] Faroese Act no. 62 of 17 May 2005 on Human Genetics Research (Act on Human Genetics Research).
[217] The official gateway to the Faroe Islands, https://www.faroeislands.fo/people-society/education-research/research-and-innovation/
[218] For ongoing projects, please refer to: http://biobank.gov.fo/?page_id=174&lang=en

In 2011 the Genetic Biobank launched the 'FarGen Project' to develop a platform for genetic research.[219] The project also aims to improve treatment of medical conditions, ideally in the form of personal medicine, and develop local expertise regarding DNA preparation for genome sequencing, including secure handling and storage of digital data from sequencing.[220]

6.4 General principles on use of health data

As in Denmark, access to Faroese health data is strictly regulated and must comply with the basic processing principles.[221]

Access to non-anonymized health data from medical records for secondary use generally requires either a written consent from the patient (the data subject) or a statutory exemption allowing access to health data for secondary use. Additionally, permits from one or more relevant authorities are required or as for health registers, approvals from one or more registry keepers. [222]

Hence, both statutory exemptions and consent provide legal basis for secondary use. As for health data, statutory exemptions are mainly placed in the Faroese health legislation which i.e. allow access to health data for an approved health scientific research project.

If no statutory exemptions provide legal basis, the patients' consent must be obtained for access to health data. The consent must comply with the conditions laid down in the data protection legislation and the health legislation. Please refer to this report section 4.3.3 and 5.4 for further on the requirements relating to the validation of a consent, as it corresponds to the requirements laid down in the GDPR and the Danish legislation.

6.5 Legislation

6.5.1 General

In the Faroe Islands, data protection is regulated by the Royal Decree on Processing of Personal Data[223] and the Faroese Personal Data Processing Act.[224]

The Royal Decree on Processing of Personal Data applies to processing of personal data in connection with activities carried out by authorities of the Kingdom of Denmark in the Faroe Islands.[225] The Faroese Personal Data Processing Act applies to activities carried out by *others,* hereunder other public and private actors in the health sector. Although the Faroese Data Protection Legislation is based on the standards set out in the Data Protection Directive, the GDPR is not implemented in Faroese Law.

The EU Commission has decided that the Faroese Personal Data Processing Act provides an adequate level of protection.[226] Thus, transfer of data to the Faroe Islands, apart from the authorities of the Kingdom of Denmark in the Faroe Islands, is considered as a transfer to a secure third country. The EU Commission has not made a similar decision regarding the Royal Decree on Processing of Personal Data. Hence, transfer to the authorities of the Kingdom of Denmark in the Faroe Islands will be regarded as transfer to a third country.

Please note that the Faroese health legislation supplements and takes precedence over the Faroese Data Protection Legislation.

6.5.2 Data Protection

The Faroese Data Protection Regulation corresponds to the Danish Data Protection Regulation. Hence, processing must comply with the basic processing principles in the Faroese Data Protection Regulation and be based on a specific legal basis in either Faroese Data Protection Regulation or special legislation. Please refer to this report section 5.5.2 for details on the basic processing principles and alternative legal bases, as these corresponds to the Danish.

Besides consent, statutory provisions may constitute legal basis for processing. For example, transfer of diagnosis information from the national health care system or health data from genealogical records to the Genetic Biobank does not require the data subject's consent.[227]

Specific regulations may further apply to personal data considered as *health data*. According to the Faroese Data Protection Legislation, health data can be processed for the sole purpose of carrying out statistical or scientific studies of significant importance to society. Depended on whether the processing is necessary to carry out these studies, or the public interests of the processing clearly overrides the interest of the data subject.[228] The data

[219] FARGEN - Faroe Genome Project. https://www.fargen.fo/en/about-fargen/public-health-services/
[220] The official gateway to the Faroe Islands, https://www.faroeislands.fo/people-society/education-research/research-and-innovation/
[221] Please refer to this report section 4.2.4 as it corresponds to the principles laid down in the GDPR.
[222] E.g. permission of a health scientific research project, unless disclosure is required e.g. by law or contract.
[223] Royal Decree no. 754 of 19 June 2017 on Commencement of the Act on Processing of Personal Data for the Faroe Islands (Royal Decree on Processing of Personal Data). The Danish DPA supervises that the royal decree is complied with.
[224] Faroese Act no. 73 of 8 May 2001 on Processing of Personal Data (Faroese Personal Data Processing Act). The Faroese DPA supervises that the act is complied with.
[225] Namely the High Commissioner of the Faroe Islands (Rigsombudsmanden), the Court of the Faroe Islands (Sorenskriveren), the Commissioner of the Faroe Islands (Politimesteren på Færøerne), the Prison and Probation Service of the Faroe Islands (Kriminalforsorgens afdeling), the Island Command Faroes (Færøernes Kommando) and the Chief Medical Officer of the Faroe Islands (Landslægen).
[226] Cf. decision from the EU Commission of 5 March 2010 (2010/146/EU).
[227] The Act on Human Genetics Research section 7 (1).
[228] The Royal Decree on Processing of Personal Data section 10 (1) and the Faroese Personal Data Processing Act section 8 (2).

cannot subsequently be processed for other purposes and can only be disclosed to a third party in possession of an approval from the supervisory authority.[229]

Further, if data is processed on behalf of the public administration under the authorities of the Kingdom of Denmark, a notification to and/or a statement from the Danish DPA are generally required. The notification must inter alia include information regarding the processing, the recipients to whom the data can be transferred, if transfer of data to third countries is intended etc.

For processing conducted by others than the authorities of the Kingdom of Denmark in the Faroe Islands, the Faroese Personal Data Processing Act provides an exhaustive list[230] of situations where health data can be processed, hereunder if;

- permission from the Faroese DPA is obtained231; and
- the processing fulfills one of the conditions in section 9 (1)232 and section 10 (1), including e.g. obtaining the data subject's explicit consent; or
- the processing is necessary for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where such personal data is processed by a health care personnel subject to statutory obligation of professional secrecy.

Processing of health data by electronic means and/or by non-automatic filling system must be approved by the Faroese Data Protection Agency.[233]

6.5.3 Professional secrecy

As in Denmark, health care personnel are subject to professional secrecy. Please refer to section 5.5.3 for details on this duty, as it corresponds to the Danish.

The duty of professional secrecy is laid down in the Faroese Health Act, and processing of health data obtained in the conduct of health care personnel's profession, including activities covered by other health legislation, will be subject to the professional secrecy.

However, Faroese legislation provides exemptions from the professional secrecy. Some of the exemptions are applicable based on a consent from the data subject, while other exemptions are applicable based on an alternative legal basis. Though, no Faroese act provides an alternative legal basis to innovators, thus the data subject's consent must be obtained for access to health data for innovation purposes.

6.5.4 General regulation on health research

The Faroese Health Act

The Faroese Health Act regulates access to health data, additional sheer private matters and other confidential information from medical records for research purposes.[234]

Corresponding to the Danish Health Act, health data may be transferred to a researcher for the purpose of an approved health scientific research project or for statistics or planning purposes after approval has been collected, without the patients' consent.[235] The term *researcher* includes both researchers with a medical or other educational background.

Hence, no legal basis for transfer of health data from medical records for the purpose of a *pure innovation project* is provided by the Faroese Health Act. Thus, innovators must obtain the data subject's consent.[236]

The Faroese Committee Act

The Faroese Committee Act regulates access to non-anonymized health data including biological material for health scientific research projects. For access to such data without the patients' consent, it is decisive that the project is in fact considered to be a research project.

Please refer to section 5.5.4 regarding the Danish Committee Act, for a definition of a health scientific research project, as Faroese definition corresponds to the Danish.

As a rule, all health scientific research projects are covered by the duty of notification and must be notified to the competent scientific ethics committee.[237] If a project is not permitted by a scientific ethics committee, access to health data requires the patient's consent.[238] If a health

[229] The Royal Decree on Processing of Personal Data sections 10 (2) and (3).
[230] Cf. associated bill of 28 February 2001 Regarding the Faroese Personal Data Processing Act, p.54. The Faroese DPA may grant permission to the processing of health data in other situations where processing is necessary due to public interests.
[231] The Faroese Personal Data Processing Act section 35 (1).
[232] The processing is subject to statutory authority or necessary for (i) the performance of a contract with the data subject, (ii) for compliance with a legal obligation, (iii) to protect the vital interest of the data subject (iv) for the performance of a task carried out in the public interest, (v) for the performance of a task carried out in the exercise of official authority, or (vi) for the purpose of the legitimate interests pursued by the controller and these interests are not overridden by the interests of the data subject.
[233] The Faroese Personal Data Processing Act section 32 (1), cf. Executive Order no. 124 of 19 September 2011 on Notification and Exemptions from Approval to Process. The notification must include information regarding the processing, a general description of the measures taken to ensure security of processing etc.
[234] The Faroese Health Act section 46.
[235] Approval of such projects are regulated by Royal Decree no. 961 of 15 July 2013 on Science Ethics Processing of Health Scientific Research Projects for the Faroe Islands (Faroese Committee Act). When a specific research project is not regulated by the Faroese Committee Act, the data may still be transferred to a researcher for a specific research project, when the project is of significant societal interest and has been approved by the Danish Patient Safety Authority.
[236] Provided that the projects are not covered by some of the other exemptions laid down in the Faroese Health Act.
[237] Though, it is a prerequisite that the research activity is conducted in the Faroe Islands, cf. the Faroese Committee Act section 15 (1).
[238] The Faroese Health Act section 46 conversely.

scientific research project includes clinical trials with medicines, it is further a prerequisite that the person responsible for the trial is qualified to make treatment-related decisions, and has a sufficient health scientific education, e.g. as a doctor, as well as clinical experience.[239] Inclusion of trial participants in clinical research requires the patient's consent, the only exception being research into acute experimental situations, which does not involve medicine testing. Consent provided in connection with participation in clinical research can always be withdrawn.

Please note that health scientific research projects using only anonymized human biological material are not subject to any notification requirements and any prior approval from a scientific ethics committee is not required.

6.6 Access to health data for secondary use

6.6.1 Access to health data in medical records

General

As in Denmark, Faroese public and private health care providers must keep manual or electronic medical records.[240] Please refer to section 5.6.1 for an overview of the requirements for the medical records, as it corresponds to the Danish legislation.

The Faroese health services use a joint digital journal and communication system, called a THS-system.[241] As all information on patients are collected in one system, the information is available for all health care personnel.

Health data in medical records are generally subject to professional secrecy. Thus, access to the medical records are dependent on either the patients' consent or an alternative legal basis.

The patient's consent and access to own medical records

Upon request, patients have a right to receive information about whether health data in medical records is being processed, when the medical records are composed and kept at public and private hospitals, clinics, etc. If health data is being processed, patients have a right to receive information of the processing purpose, the recipients of the data, and information regarding the origin of the data.[242][243]

Access to medical records may be given by review of the records at the place of treatment, by transcript or copy to the patients.

> *Innovators cannot get access to health data from medical records without the patients' consent.*

Access to health data in medical records for health scientific research projects

Health data in medical records can be disclosed to a researcher for an approved health scientific research project, without the patient's consent.[244]

Firstly, health data can be disclosed if the project is characterized as a health scientific research project in accordance with the Faroese Committee Act. Please refer to section 5.5.4 for details on what is required to be characterized as a health scientific research project. Please note that the Faroese legislation does not provide for any explanations to differ between research and innovation.

Secondly, health data can be disclosed for a specific research project of significant societal importance, when permitted by the Danish Patient Safety Authority.[245] The Danish Patient Safety Authority will determine whether the project is of significant societal interest as well as the terms of disclosure.-Please refer to section 5.6.1 regarding the health care personnel's responsibility for collecting the disclosed information as well as permission for subsequent inquiries to the individuals in question.

Thirdly, such data can be disclosed for statistic or planning purposes when permitted by the Danish Patient Safety Authority. This permission is not required when disclosure of the data is required by law.

Data collected for the use of scientific, statistics or planning purposes, may not later be processed for other purposes. Publication of the collected information may only happen in a way where the data cannot be linked to the individuals.[246]

---

[239] The Faroese Committee Act section 21 (1).
[240] The Royal Decree no. 1472 of 16 December 2013 on Authorization of Health care Personnel and on Health Professional Business for the Faroe Islands as Amended by Royal Decree no. 994 of 2 July 2018 on amendment of the Act on Authorization ("Faroese Authorization Act"), chapter 6.
[241] The Faroese Ministry of Health on the digital health service: https://www.hmr.fo/en/what-we-do/health-and-prevention/the-digital-health-service/
[242] The Faroese Health Act section 37 (1).
[243] In specific cases, patients have a right to refuse others from accessing their medical records, for example health care personnel's collection of health data in connection with treatment.
[244] The Faroese Health Act section 46.
[245] When the project is not subject to the scope of the Faroese Committee Act, the Danish Patient Safety Authority permits the project in accordance with the Faroese Health Act section 46 (2).
[246] The Faroese Health Act section 48.

Access to health data in medical records for other purposes

Health care personnel can with the patient's consent disclose information regarding the patient's health to other health care personnel, authorities, organizations, private individuals and others.

Information can also be disclosed *without the patient's consent* when disclosure is;

1. required by law and the information is of essential importance for the receiving authority's case handling;
2. necessary for legitimate protection of a public interest or of significant concern to the patient, health care personnel or others; or
3. necessary for an authority to carry out supervisory and control tasks.

It is the health care personnel in possession of the confidential information who determines whether disclosure is justified in the specific case.

Innovation purposes are not covered by any of these exemptions, thus *disclosure of data to innovators requires the patients' consent*.

6.6.2 Access to health data in national health registries

As a rule, all health scientific research projects must be approved by a scientific ethics committee. However, health scientific registry research projects that only includes statistics, and anonymized data, do not require approval. If such projects contain a significant element of biomedical research, including non-anonymized human biological material, the projects must be submitted to a scientific ethics committee for approval.[247]

In general, the same rules apply to surveys and interviews as for health scientific registry research projects, i.e. surveys and interviews must be filed with a scientific ethics committee if non-anonymized human biological material is included.[248] If health data is requested for a project from both registers and medical records, prior approval from the Danish Patient Safety Authority must be obtained.[249]

Access to health data from registers requires submission of an application to the registry keeper in question.

6.6.3 Access to health data from Statistics Faroe Islands

Statistics Faroe Islands is the national statistical authority of the Faroe Islands and is an independent authority placed under the Faroese Ministry of Finance.

Statistics Faroe Islands has different data relating to the Faroese population gathered in their data bank (Statbank).[250] The data bank provides access to online retrieval of data relating to health.

Researchers and others may obtain access to *anonymous microdata* from Statistics Faroe Islands under certain conditions. Such access can be applied for via email.[251]

6.6.4 Access to health data in biobanks

General

A biobank is considered a manual register in accordance with the Faroese Data Protection Legislation. Please refer to section 5.6.4 for further on the regulation of a biobank as well as the distinction between a research and a clinical biobank.

Biological material submitted by a patient in connection with treatment can as rule be transferred for use in an approved health scientific research project without the patient's consent. However, the patient may prohibit use of his/her biological material for purposes other than treatment.[252]

The Genetic Biobank manage the FarGen Project. In order to access data from the FarGen Project, necessary authorizations from the Gene Collection, the Faroese Scientific Ethics Committee and the Faroese Data Protection Agency must be obtained.[253]

> *Access to biological material stored in the Genetic Biobank requires a contractual research agreement with the Genetic Biobank.*

Access to health data and biological material from the Genetic Biobank

In the Faroe Islands, the Genetic Biobank contains anonymous data from the tissue register, the diagnosis register, and the genealogy register, and it is organized, developed and administered by the Gene Collection.

[247] The Faroese Committee Act section 14 (2).
[248] L.c.
[249] The Faroese Health Act section 46 (2).
[250] Statbank, access to statistical data, https://statbank.hagstova.fo/pxweb/en/H2/
[251] Statistics Faroe Islands, access to anonymous microdata, https://hagstova.fo/en/access-anonymous-microdata

[252] The Faroese Health Act. The Faroese authorities can use the Danish Registry Regarding Use of Tissue (see this report section 5.6.4). For further information: https://www.logting.fo/files/casestate/16813/087.16%20Skjal%202.%20Almindelige%20og%20saerlige%20bemaerkninger%20til%20kongelig%20anordning%20for%20Faeroerne%20sundhedsloven.pdf
[253] FARGEN - Faroe Genome Project, https://www.fargen.fo/en/about-fargen/structure/genetic-biobank-of-the-faroe-islands/

Access to health data in the Genetic Biobank is regulated by the Act on Human Genetics Research.

The Gene Collection has the authority to enter into agreements regarding the study of information contained in the biobank's registers.[254] Human genetics research related to the human tissue of individuals registered in the Faroe Islands can only be conducted by those entities that have entered into a contractual research agreement with the Gene Collection.[255]

In connection with the contractual research agreements, the Gene Collection is authorized to transfer the necessary biological material and personal data to a research project for study.[256] The biological material and personal data may only be used for the agreed.

As a rule, consent is needed for accessing genetic information.

Access to health data for health scientific research projects with clinical trials

A health scientific research project including clinical trials with medicines or medical equipment requires that the responsible for the trial is qualified to make treatment related decisions and has an appropriate health scientific education and clinical experience.[257]

Inclusion of trial participants in clinical research requires the participant's consent in general.[258] Please refer to this report section 5.6.4 on access to data based on the provided consent, including withdrawal of such consent, as it corresponds to the Danish.

However, it is possible to apply for a dispensation from the required consent if the project is not considered to involve risk or in any other way be at strain for the trial participant.[259]

6.6.5 Access to health data in public archives

General

All information in the Faroese State Archive shall be available for public and private institutions and researchers. The Faroese State Archive can alone or in collaboration with others perform research regarding the information.

The Faroese Home Rule Government and governmental authorities must submit their archive units to the Faroese State Archive when they reach 30 years of age. Thus, the units become accessible for everyone.[260] Archives containing personal data is excluded from this rule and become accessible after 80 years.[261]

The chairman of the Home Rule Government may, after statement from the Faroese Data Protection Agency, determine further rules regarding storage of archive units covered by the Faroese Personal Data Processing Act in public archives.[262]

In specific cases, the Faroese State Archive can grant access to archive units or groups of these before 80 years have passed.[263] Whoever gets access to use of non-immediately accessible records may not unjustified publish, transfer or exploit confidential information, including health data obtained in connection with the access, though copying is permitted.[264] However, copies cannot be transferred or publicly disclosed without specific permission from the Faroese State Archive.[265]

Archive units containing health data are accessible upon 80 years of age. However, such units can be accessed earlier when permission from the relevant institution is obtained.

[254] The registers contain anonymized data that is only accessible for the Genetic Biobank. When negotiating an agreement regarding human genetics research, the Gene Collection must ensure that the agreement is governed by Faroese law and that the legal jurisdiction stipulated in the agreement is that of the Faroe Islands and Denmark, cf. the Act on Human Genetic Research section 3 (4).
[255] The Act on Human Genetics Research section 4 (1). Contractual research agreements must require that a responsible clinician is associated with the research project.
[256] Ibid section 5 (1).
[257] The Faroese Committee Act section 21 (1).
[258] Except for research into acute experimental situations in trials.
[259] The Faroese Committee Act section 10.
[260] The Act no. 49 of 28 April 1992 on the Faroese State Archive as amended by Act no. 63 of 30 April 2018 on Amendment of the Act on the Faroese State Archive (Faroese Archive Act), section 8 (1) and 11 (1).
[261] The Faroese Archive Act section 13 (1). The accessibility deadline is calculated from the archive unit's end year, cf. the Faroese Archive Act section 14.
[262] The Faroese Archive Act section 7a.
[263] Ibid. section 15 (1)- (3).
[264] The Faroese Archive Act section 16.
[265] The Executive Order no. 117 of 5 July 1995 on Public Archives section 11, which lay down further rules regarding the accessibility and the conditions regarding use of the accessible information.

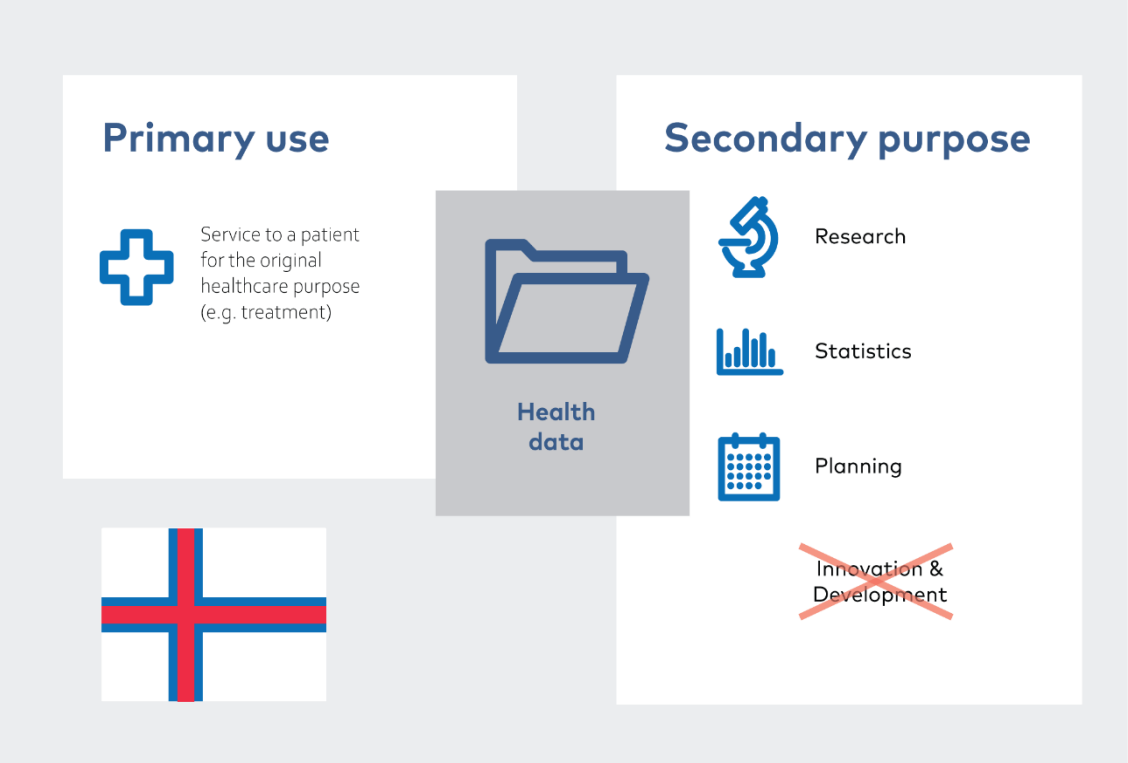


Figure 4 - Regulated division of primary and secondary use of health data in the Faroe Islands

6.7 Transfer of and transborder access to health data

6.7.1 General principles in the Faroese Data Protection Legislation

The Royal Decree on Processing of Personal Data

According to the Royal Decree on Processing of Personal Data, data covered by the act can generally be transferred outside the EU and the EEA provided that the country in question provides an adequate level of protection.[266] Transfer to third countries not providing an adequate level of protection requires that special exemptions are applicable, as explicit consent from the data subject.

Hence, transfer of health data is possible to the other countries or self governing territories in the Nordic region. Greenland is excluded in this regard, as it is a third country not recognized to provide an adequate level of protection. Thus, transfer to Greenland requires that additional requirements are met.[267]

The Faroese Personal Data Processing Act

Under the Faroese Personal Processing Act, the Nordics are considered foreign countries. Thus, approval from the Faroese DPA is generally required to transfer personal data.[268] For transfer of personal data, the foreign country must ensure an adequate level of protection.[269]

An exception is made for transfer of sensitive data[270], including health data, which can be transferred to an exhaustive list of countries, including Denmark, Finland, Iceland, Norway and Sweden without approval. Transfer to these countries merely requires notification of the transfer to the Faroese DPA.[271] For transfers to Åland and Greenland, both notification to and approval from the Faroese DPA is required.

Further, the Faroese DPA may also authorize transfers of personal data to countries not providing an adequate level of protection. For such authorization, the following requirements must be met[272];

1. the data subject has given his consent to the transfer[273];

[266] The Royal Decree on Processing of Personal Data section 27.
[267] Ibid. section 27 (3).
[268] The Faroese Personal Data Processing Act section 16 (1), cf. section 35 (6).
[269] Ibid. section 16 (1).
[270] As covered by the Executive Order on Notification and Exemptions from Approval to Process.
[271] In accordance with Executive Order no. 31 of 21 March 2019 on Transfer of Personal Data to Foreign Countries and the Executive Order on Notification and Exemptions from Approval to Process section 2 (2), transfer of personal data to foreign countries without permission from the Faroese DPA requires notification.
[272] The Faroese Personal Data Processing Act section 17 (1).
[273] The consent must be given in accordance with the Faroese Personal Data Processing Act section 2 (8).

2. the transfer is required by international conventions or because of membership in an international community;
3. the transfer is necessary for the performance of a contract with the data subject or to do what is required, to implement pre-contractual measures taken in response to the data subject's request;
4. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject with a third party;
5. the transfer is necessary in order to protect the vital interest of the data subject;
6. the transfer is necessary in order to identify, submit in to force or protect a legal claim;
7. the transfer is necessary or legally required on important public interest grounds; or
8. statutory authority exists when data is required from a public registry.

The Faroese DPA may authorize a transfer of personal data to a foreign country that does not comply with the above, when the data controller presents adequate safeguards with respect to the protection of the rights of the data subject.

6.7.2 Special regulation regarding transfer of health data

Section 49 in the Danish Health Act is not implemented by the royal decree for the Faroe Islands. Thus, at the time of this report, transfer of health data to third countries is not regulated specifically in the Faroese health legislation. Hence, health data can be transferred in accordance with the general rules in the Faroese Data Protection Legislation.

In the absence of statutory provisions, both consent from the data subject and necessary authorization from authorities, may constitute legal basis for such transfers.

6.8 National obstacles

As in Denmark, the Faroese legislation provide legal basis for access to health data for research purposes without the patients' consent upon the fulfilment of certain conditions but does not provide such legal basis for innovation purposes. Furthermore, the Faroese information resources are also decentralized and no shared entrance to all available health data exists.

The Faroese legislation and specially the information resources are not as advanced and extended as in Denmark. Regardless, it is still the same obstacles as related to existing Danish legislation and system of information resources that are present in the Faroe Islands.

7. Greenland

7.1 Introduction

As in Denmark and the Faroe Islands health data is firmly regulated under Greenlandic Law.

Generally, health care personnel are subject to professional secrecy and must treat information on patients' health conditions confidential. However, there are exemptions to the professional secrecy which provide legal basis for access to non-anonymized health data for secondary use.

The legislation neither refers to nor address access to health data for *innovation* purposes explicitly. Hence, access to non-anonymized health data for the purpose of innovation must as a rule be based on *consent* from each data subject if not covered by an exemption for any other secondary purpose.

When legal basis is obtained, the relevant health data may be applied for. No shared entrance to all health data exists. In certain cases, the application process consists of several steps and permits from different authorities may be required. As the existing legislation does not provide legal basis for such shared entrance, nor access to health data for innovation purposes without obtaining consent, it is difficult for innovators to access non-anonymized health data in Greenland.

In terms of transborder access, health data can generally be transferred across the Nordics on similar grounds as processing within Greenland. Though, the authorities of the Kingdom of Denmark in the Faroe Islands constitute an exception, as they are not subject to legislation providing the required adequate level of protection. The Greenlandic health legislation only address transfer to authorities outside of Greenland, private operators are not included. This may indicate that the legislator did not intend health data to be transferred to private companies, etc. outside Greenland.

7.2 Greenlandic health care system and information resources

The Greenlandic health care system is placed under the Greenlandic Department of Health, which is the supreme health care authority of Greenland. The Greenlandic health care system is administrated by the Greenlandic Health and Prevention Authority.

Similar as under Danish law, health data is collected by health care personnel when providing health care and recorded in medical records. Access is given to both health care personnel and the concerned patient. In addition to medical records, health data is stored in various registries and biobanks, as the Statistics Greenland, the Greenlandic Biological Biobank, the Danish Civil Registration System[274] Registry and Denmark's National Biobank that also contains data regarding Greenlandic citizens.[275]

As for the Faroe Islands, Greenland has limited information resources within the health care sector, presumably due to the limited size of their health care institutions.

As in Denmark and the Faroe Islands, there is no central entrance to all stored health data. Access is dependent on the type of data, what type of register/biobank the data is stored in, and who the registry keeper is.

Relevant authorities authorized to approve access to health data for secondary use, are the Statistics Greenland, CAHME and Denmark's National Biobank. Access to the registries and biobanks may also depend on approval from the Danish DPA and the Greenlandic Scientific Ethics Committee[276] (or the Office of the Chief Medic[277]).

7.3 Legal reforms enabling secondary use

As in Denmark and the Faroe Islands, health strategies and legal reforms regarding secondary use of health data have addressed access for research purposes, and not innovation purposes specifically.

In 2019, the member of the Greenlandic government responsible for health engaged in a registry collaboration with the Danish State's Serum Institute with the purpose of systematizing Greenlandic biobank data. At the time of this report, no collaboration terms for access to collected material appear to have been defined.

---

[274] About Centralt Personregister, https://www.danishhealthdata.dk/find-sundhedsdata/CPR-registeret

[275] Biobank skal rumme hele Danmarks befolkning, Videnskap.dk (2012): https://videnskab.dk/krop-sundhed/biobank-skal-rumme-hele-danmarks-befolkning

[276] The Greenlandic Scientific Ethics Committee oversees that scientific studies are conducted in accordance with the guidelines laid down in the Danish Committee Act, and disclosure of health data in relation to such studies may depend on their approval of the scientific project.

[277] For further on the Office of the Chief Medic: https://naalakkersuisut.gl/da/Naalakkersuisut/Departementer/Landslaegeembedet

Pursuant to the Strategy Plan for the Institute of Health Services and Health Science 2019-2023[278], research is one of two main tasks of the Institute of Health Services and Health Science.

With the vision of improving the health conditions in Greenland through initiatives and coordination of health research, the Greenlandic Health Research Center[279] was initiated.

The purpose of the initiative is to facilitate and strengthen the collaboration between foreign scientists and health care personnel in Greenland. The Greenlandic Health Research Center will in the long-term work for the establishment of a data archive and archive of material collected in Greenland.[280]

7.4 General principles on use of health data

As health data constitutes a distinctive and particularly sensitive category of personal data, it is as in Denmark and the Faroe Islands firmly regulated under Greenlandic Law.

As mentioned above, health data is collected by health care personnel and is stored in medical records. As a rule, health care personnel are subject to professional secrecy and must treat information on patients' health conditions confidential. Thus, access to health data for secondary use is limited and require a legal basis.

Access to non-anonymized health data from medical records for secondary use generally requires either a written consent from the patient whose data is being disclosed (the data subject) or a statutory exemption allowing access to health data for secondary use, typically combined with approvals from one or more relevant authorities[281] or registry keepers. Please refer to this report section 4.3.2 for further on the requirements relating to the validation of a consent, as it corresponds to the requirements laid down in the GDPR and the Danish legislation, except from the age restriction, which is not applicable in Greenland.

7.5 Legislation

7.5.1 General

On Greenland, data protection is regulated by the Greenlandic Personal Data Processing Act.[282]

The Greenlandic Personal Data Processing Act applies to all processing of personal data, in both public and private sector. Under the act, the data subject has a right to get confirmation from the data controller on whether the data subject's personal data is being processed. If the data is being processed, the data subject shall be provided information of the processing purpose, the recipients etc.[283] However, this does not apply when information is processed for scientific purposes or is stored in a period to prepare statistics.[284]

Access to personal data is also regulated by the Greenlandic health legislation, which supplements and shall take precedence over the Greenlandic Personal Data Processing Act.

7.5.2 Data protection

In relation to processing of personal data, the Greenlandic Personal Data Processing Act corresponds to the Danish Data Protection Regulation and the Faroese Data Protection Regulation.

Thus, processing must comply with basic processing principles in the Greenlandic Personal Data Processing Act and be based on a specific legal basis or special legislation. Please refer to this report chapter 4 for details on what are considered basic processing principles and legal basis.

According to the basic processing principles, processing must be conducted in accordance with the purpose for collecting the personal data. However, as in Denmark and the Faroe Islands, certain exceptions are laid down in the Greenlandic Personal Data Processing Act. Processing is not to be considered incompatible with the purpose of collection if processed for historical, statistical or scientific purposes,[285] or when processing is for the sole purpose of carrying out statistical or scientific studies of significant importance to society and where such processing is necessary to carry out these studies.[286] Data cannot be subsequently processed for other than these scientific or statistical purposes[287], and may only be

[278] Strategiplan for institut for sygepleje- og sundhedsvidenskab, Forskningsstrategi ved Institut for Sygepleje- og Sundhedsvidenskab, 2019-2023: https://da.uni.gl/forskning/strategiplan-for-institut-for-sygepleje-sundhedsvidenskab.aspx
[279] The Greenlandic Center of Health Research at the Institution of Health Services and Health Science (Greenlandic Health Research Center).
[280] Greenland Center for Health Research (GCHR) at the Institute of Nursing & Health Science, https://uk.uni.gl/research/greenland-center-for-health-research.aspx
[281] E.g. permission of a health scientific research project, unless disclosure is required e.g. by law or contract.
[282] Royal Decree no. 1238 of 14 October 2016 on commencement of the Danish Act no. 429 of 31 May 2000 on Processing of Personal Data as amended by act no. 1245 of 18 December 2012 for Greenland (Greenlandic Personal Data Processing Act). The original Danish Act on Processing of Personal Data (now dissolved) was implementing Directive 95/46/EC (now dissolved).
[283] The Greenlandic Personal Data Processing Act section 31 (1).
[284] Ibid. section 32 (3).
[285] Ibid. section 5 (2).
[286] Ibid. section 10 (1).
[287] Ibid. section 10 (2).

disclosed to third parties upon approval from the supervisory authority.[288]

Further, for processing conducted on behalf of the public administration or on behalf of a private data controller,[289] the Danish DPA must be notified, and a statement must be obtained.[290]

Upon transfer of health data to a third country[291] conducted on behalf of a private data controller, the Danish Data Protection Agency's prior *approval* must be obtained.[292]

7.5.3 Professional secrecy

As in Denmark and the Faroe Island, health care personnel are subject to professional secrecy. Please refer to this report section 5.5.3 for details on this duty, as it corresponds to the Danish.

The duty of professional secrecy is laid down in the Greenlandic Regulation on Patients' Legal Position. Exceptions are reliant on consent of the data subject or alternative legal basis. Certain exceptions follow from the Greenlandic legislation for research purposes. However, for innovation purposes, no alternative legal basis applies unless the specific project can be characterized as a biomedical research project, why the patients' consent must be obtained.

7.5.4 General regulation on health research

The Greenlandic Regulation on Patients' Legal Position

The Greenlandic Regulation on Patients' Legal Position regulate access to health data from medical records for research purposes.[293] This includes access to additional sheer private matters and other confidential information.

Without the patients' consent, data may be transferred to a researcher for the purpose of an approved biomedical research project.[294] All projects including health data must be subject to a scientific ethics evaluation performed by the Greenlandic Scientific Ethics Committee, who ensures that the project's purpose and methodology represents good scientific standards and that there are sufficient reasons for completing the project.[295]

Further, health data may be transferred to researchers for the purpose of statistics or planning. Such transfers are dependent on approval from the Office of the Chief Medic. Under the act, the term *researcher* includes both researchers with a medical or other educational background.

Thus, the act does not provide legal basis for transfer of health data from medical records for the purpose of a *pure innovation project*. In these circumstances, the data subject's consent is required.

Rules of Procedure for the Greenlandic Scientific Ethics Committee

The Rules of procedure for the Greenlandic Scientific Ethics Committee regulates access to health data and biological material for biomedical research projects. On Greenland, at the time of this report, there is no statutory regulation of biomedical research projects like e.g. the Danish Committee Act. However, the Greenlandic Scientific Ethics Committee must assess research projects in accordance with the Danish Committee Act.[296]

All research projects must be approved by the Greenlandic Scientific Ethics Committee. A trial protocol must be enclosed the notification of the project, and the research/trial cannot be initiated before approval is obtained.[297]

Guidelines on Health Research

For research projects conducted within the health care administration or in collaboration with such personnel, access to health data and biological material for a biomedical research project is further regulated by the Guidelines on Health Research.

Approval for such research projects must be registered with the Greenlandic Health and Prevention Authority, after approval from the Greenlandic Scientific Ethics Committee is obtained. In addition to the approval and associated material, a memorandum including information about the collaboration, the time frame for the project, etc. must be enclosed the registration.

Use of registers within the health care sector must be approved by the Greenlandic Health and Prevention Authority, and projects containing registry data cannot be initiated before such approval is obtained.

---

[288] Ibid. section 10 (3).
[289] The notification must include information regarding the processing, the recipients to whom the data can be transferred, if transfer of data to third countries is intended etc., cf. the Greenlandic Data Protection Act chapter 12 and 13.
[290] For further, see the Greenlandic Data Protection Act section 47 (2).
[291] The Greenlandic Data Protection Act section 27 (1) and 27 (3) (2-4).
[292] Ibid. section 50 (2).
[293] The Greenlandic Regulation on Patients' Legal Position section 29.
[294] Approval of such projects must be performed in accordance with the Guidelines of 8 August 2015 on Health Research and Research by the Health care Administration's Institutions prepared by the Department of Health in collaboration with the Greenlandic Health and Prevention Authority (Guidelines on Health Research) as well as the rules of procedures for the Greenlandic Scientific Ethics Committee.
[295] Cf. associated bill no. 26 of 2001 regarding the Greenlandic Regulation on Patients' Legal Position.
[296] Cf. the rules of procedure for the Greenlandic Scientific Ethics Committee. For further information on the rules laid down in the Danish Committee Act, see this report section 5.5.4.
[297] The rules of procedure for the Greenlandic Scientific Ethics Committee section 7.

7.6 Access to health data for secondary use

7.6.1 Access to health data in medical records

General

As in Denmark and the Faroe Islands public and private health care providers on Greenland must keep manual or electronic medical records. A medical record must be kept for each patient and the record must contain information necessary for providing a good and secure patient treatment. Information included must be readable and cannot be deleted.

The medical records are primarily stored electronically. The Greenlandic health care services uses a joint EPJ-system, thus all information on patients are collected by one system and thereby available for all health care personnel across regions.

Health data in medical records are in general subject to the professional secrecy, which means that access is reliant on either the patient consent or an alternative legal basis. Thus, professional secrecy may also hinder access to health data.

Innovators cannot access health data from medical records without the patients' consent.

The Patient's Consent and Access to Own Medical Records

Upon request, patients have a right to access own medical records composed by health care personnel and kept at hospitals, clinics etc.[298]

Access to medical record may be by review of the medical records at the place of treatment, by transcript or copy of the medical record.[299]

Patients may also get access to own health data, including course of treatment, medicine, lab results, etc. A patient must request access of right to the health care institution that has treated the patient.[300]

Access to health data in medical records for biomedical research projects

On Greenland, health data from medical records can without the patient's content be disclosed to a researcher for a specific biomedical research project on prevailing terms.[301] Health data includes additional sheer private matters and other confidential information.

A biomedical research project must be approved by the Greenlandic Scientific Ethics Committee. Thus, health-related research projects including personal data from residents of Greenland must be approved, regardless of the source of information, e.g. registries, clinical studies or biological material. The approval requirement also applies for new analysis of data already collected (due to purpose limitation).

Approval of a biomedical research project including register data (besides from data in medical records) from the health care sector, requires further approval from the Greenlandic Health and Prevention Authority. Further, the Greenlandic Health and Prevention Authority must be notified of all research projects that take place in institutions of the health care administration or in collaboration with personnel within the health care administration.[302]

Subsequent inquiries to the individuals, whose medical records have been collected, etc. may only be made to the extent permitted by the health care personnel who have treated the concerned individuals. For examples, the treating health care personnel may permit inquiries from researchers who use information from medical records to find qualified participants to a clinical research study or a survey.

Health data, additional sheer private matters and other confidential information from medical records may also be disclosed for the use of statistic or planning when permitted by the Office of the Chief Medic.[303]

Approval regarding the above is not required when disclosure of the data is required by law.

Data collected for the use of scientific work, statistic or planning may not later be processed for other than scientific, statistical planning purposes. Publication of the collected information as well as research results may only happen in a way where the information cannot be ascribed to private individuals.

Scientists can access health data for the purpose of approved biomedical projects or for the use of statistics or planning without the patient's consent.

[298] The patient must request the right of access. cf. the Greenlandic Regulation on Patients' Legal Position section 20 (3).
[299] The Greenlandic Regulation on Patients' Legal Position section 21 (2).
[300] Peqqik.gl, Din sundhed på nettet.
[301] The Greenlandic Regulation on Patients' Legal Position section 29.
302 Cf. the Guidelines on Health Research.
303 The Greenlandic Regulation on Patients' Legal Position section 30 (1).

Access to health data in medical records for other purposes

With the patient's consent, health care personnel can disclose information regarding the patient's health and other confidential information to other health care personnel, authorities, organizations, private individuals and others for non-treatment purposes.

Notwithstanding the above, disclosure *does not require the patient's consent* when the disclosure is;[304]

1. required by law and the information is of essential importance for the receiving authority's case handling;
2. necessary for legitimate protection of a public interest or of significant concern to the patient, health care personnel or others; or
3. necessary for an authority to carry out supervisory and control tasks.

The health care personnel in possession of confidential information determines whether disclosure according to the above is justified.

Innovation purposes are not covered by the exemption, thus disclosure of data to innovators requires the patients' consent.

7.6.2 Access to health data in national health registries

If a registry research project only includes statistics and anonymized data, approval of the project is not required.

However, if the registry research project also contains a significant element of biomedical research, including non-anonymized human biological material, the project must be submitted to a scientific ethics committee for approval.[305]

In general, the same rules apply to surveys and interviews as for registry research projects, i.e. surveys and interviews must be filed with the Greenlandic Scientific Ethics Committee if human biological material is included.

Access to health data from registries requires submission of an application to the relevant registry keeper in question.

Access to health data from Statistics Greenland

Statistics Greenland is the national statistical authority in Greenland and is an independent authority under the Ministry of Finances.

Statistics Greenland has different data relating to the Greenlandic population gathered in its data bank (Statistikbanken).[306] The data bank provides access to online retrieval of data relating to health.

The data may be transferred for the purpose of research if necessary for the completion of the research in question.[307] The data may only be transferred as non-identifiable data.

7.6.3 Access to health data in biobanks

Biobanks are regulated by both data protection legislation and health legislation.

A biobank is regarded as a manual registry in accordance with the Greenlandic Personal Data Processing Act.

The Greenlandic Ethics Committee assess biomedical research projects in accordance with the provisions laid down in the Danish Committee Act. Thus, as a rule, use of biological material in a biomedical research project requires notification to and approval from the Greenlandic Scientific Ethics Committee.

Biomedical research projects including only anonymous human biological material does not require notification to and approval from a scientific ethics committee.

The requirements for access to data regarding Greenlandic citizens from Denmark's National Biobank is described above in section 5.6.4.

> *Foreign scientists can get access to material from the Greenlandic Biological Bio-bank under certain conditions, but without the patients' consent.*

Access to health data and biological material from the Greenlandic Biological Biobank

Biological material in the Greenlandic Biological Biobank[308] is stored for further analysis, etc.

304 Ibid section 26 (2).
305 Cf. the rules of procedures for the Greenlandic Scientific Ethics Committee, cf. the Danish Committee Act section 14 (2).
306 Public authorities and institutions must provide information requested by the Statistics Greenland, necessary for the preparation of statistics, cf. Home Rule Act no. 11 of 29 October 1999 on Statistics Greenland (Act on Statistics Greenland) as amended by Act no. 36 of 9 December 2015 on amendment of the Act on Statistics Greenland (Amendment Act on Statistics Greenland), Statbank Greenland, http://bank.stat.gl/pxweb/da/Greenland/Greenland__SB
307 The Amendment Act on Statistics Greenland section 2.
308 The Greenlandic Biological Biobank is placed at the Center of Arctic Health & Molecular Epidemiology, Department of Public Health, Aarhus University (CAHME).

CAHME is responsible to the Danish Data Protection Agency, the Greenlandic Scientific Ethics Committee and the Danish Health Authority regarding information from medical records.

The steering group of the Greenlandic Biological Biobank assess applications for approval of scientific projects[309] where the biological databank is included as source of data. The steering group must ensure that disclosure fulfills current demands from the Danish DPA and the Greenlandic Scientific Ethics Committee, etc.[310]

Material from the Greenlandic Biological Biobank can within the scope of Danish legislation[311] be made accessible for foreign scientists for scientific purposes and the steering group can under provision of the rules laid down in the Danish Data Protection Legislation[312] give foreign scientists right of use to the material. Apart from that, innovators may not access the biological material for innovation purposes.

Access to health data for the purpose of clinical trials

In general, inclusion of clinical trials in research projects are not regulated to the same extend as in e.g. Denmark. However, the Greenlandic Scientific Ethics Committee assess projects in accordance with the Danish Committee Act,[313] thus inclusion of trial participants requires consent. However, it is possible to apply for a dispensation from the required consent if the project is not considered to involve risk or in any other way be at strain for the trial participant.

A consent to participate can always be withdrawn without harm of the concerned participant. A withdrawal will not affect the processing of personal data regarding the concerned participant that already has been included in the project.

7.6.4 Access to health data in public archives

Greenlandic archive units containing information regarding individuals' private conditions, including health data, are accessible when they reach 80 years of age.[314]

The public institution who has submitted the archive, after deliberation with the Greenlandic National Museum and Archive, may determine a longer accessibility deadline when significant consideration to protection of public or private interests calls for it.[315]

For research purposes, the Greenlandic National Museum and Archive can make exemptions to the above.[316] An exemption regarding access to archive units for which a longer accessibility deadline is determined, requires prior approval from the delivering authority.[317]

The Greenlandic National Museum and Archive may approve loan of records for the use in libraries, approved museums or similar institutions for research purposes. However, loan to private individuals is not permitted.[318]

Whoever gets access to use of records that are not publicly accessible may not unjustified publish, transfer or exploit confidential information[319], including health data, obtained in connection with the access.[320]

> *Archive units that contain health data are accessible upon 80 years of age. However, exemption can be made by the Greenlandic National Museum and Archive for access for research purposes.*

[309] Projects must have been approved by a scientific ethics committee prior to the application for biological material from the biobank.
[310] Cf. the bye-laws of the steering group of the Greenlandic Biological Biobank at CAHME as revised on 22 November 2019.
[311] Since the material from the Greenlandic Biological Biobank is stored in Denmark and therefore subject to Danish legislation.
[312] The bye-laws refer to the dissolved Danish Act on Processing of Personal Data but may be understood as the existing Danish Data Protection Act and the rules laid down regarding disclosure of data, including section 31.
[313] Cf. the rules of procedures for the Greenlandic Scientific Ethics Committee.
[314] The Greenlandic Act no. 5 of 3 June 2015 Regarding Archives ("Greenlandic Archive Act") section 16. The accessibility deadline is calculated from the archive unit's end year, cf. the Greenlandic Archive Act section 22.
[315] Ibid. section 22.
[316] Ibid. section 20 (1).
[317] Ibid. section 20 (2).
[318] Cf. the preparatory work of the Greenlandic Archive Act.
[319] According to the preparatory work of the Greenlandic Archive Act information is confidential when characterized as confidential by law or other valid clause, i.e. health data is confidential data, cf. the data protection legislation and the health legislation.
[320] The Greenlandic Archive Act section 22.

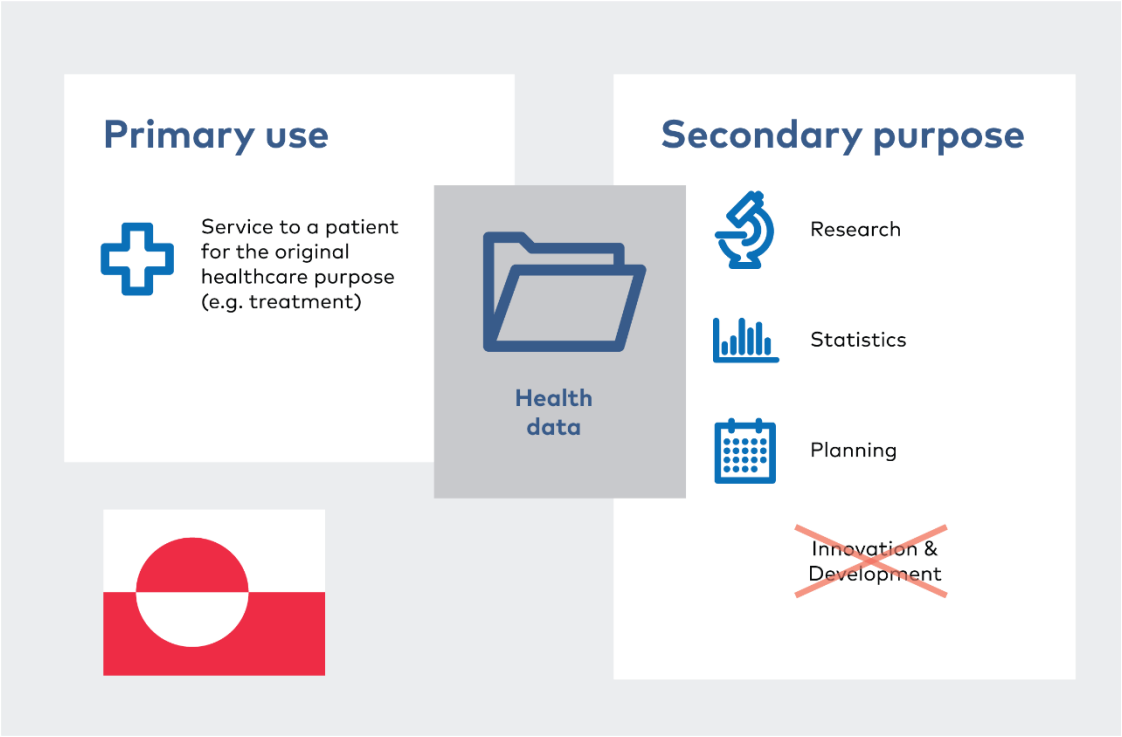


Figure 5 - Regulated division of primary and secondary use of health data in Greenland

7.7 Transfer of and transborder access to health data

7.7.1 General principles in the Greenlandic Personal Data Processing Act

As a rule, data can only be transferred to third countries (outside the EU and EEA) if the third country ensures an adequate level of data protection.[321]

Transfer to third countries not providing an adequate level of protection requires e.g. the data subject's consent, that transfer is required by law or other special exceptions. Personal data may also be transferred if the transfer is based on the standard-contract clause approved by the EU Commission. Also, the Danish DPA can approve transfer where none of the abovementioned requirements are met, if the data controller provides adequate guarantees for protection of the data subject's rights.

For transfer of health data to third countries conducted on behalf of a *private data controller*, the Danish Data Protection Agency's prior *approval* must be obtained.[322]

The Kingdom of Denmark on the Faroe Islands is not recognized as providing an adequate level of protection. Thus, such transfers are only permitted when at least one of the abovementioned exceptions are met. However, for transfer to the Faroe Islands *others than* authorities of the Kingdom of Denmark, including public and private operators, adequate protection is considered provided.

7.7.2 Specific regulation regarding transfer of health data

Health data can be transferred to other Nordic authorities if the requirements in the Greenlandic Personal Data Protection Act and the health legislation are met.

The Greenlandic Home Rule Government can – but has not - lay down detailed rules for transfer of health data to *authorities* outside of Greenland.[323] Private operators are not included, and transfer to private operators outside of Greenland does not seem to be further regulated. This may immediately suggest that it has not been the legislator's intention, that health data could be transferred to private companies, etc. outside of Greenland.

7.8 National obstacles

As in Denmark and the Faroe Islands, the Greenlandic legislation provide legal basis for access to health data for research purposes without the patients' consent upon the

[321] The Greenlandic Personal Data Processing Act section 27.
[322] The Greenlandic Data Protection Act section 50 (2).
[323] The Greenlandic Regulation on Patients' Legal Position section 32.

fulfilment of certain conditions but does not provide such legal basis for the purpose of innovation explicitly. Furthermore, the Greenlandic information resources are decentralized and no central entrance to all available health data exists.

Corresponding to the Faroe Islands, the Greenlandic legislation and specially the information resources are not as advanced and extended as in Denmark. Greenland has smaller sized institutions and more limited financial resources for providing data and statistics and are also in lack of a national data catalogue. Regardless, still the same obstacles as related to the existing Danish legislation and system of information resources are present in Greenland.

8. Finland

In May 2019, Finland adopted specific legislation regarding secondary use of health and social data.

8.1 Introduction

In May 2019, Finland became the first Nordic country to adopt an act on secondary use of health and social data, enabling regulated secondary use of health and social-related information and providing a one-stop permit and data shop for secondary use purposes.

Although access to health and social data remains subject to regulations and legal limitations in Finland, the national legislation enables effective and secure processing of personal data collected and stored in connection with Finnish health care and social welfare activities.

The Act on the Secondary Use of Health and Social Data came into force on 1 May 2019, and in January 2020, Findata, a separate social and health data permit authority, started its operations.[324] Findata is placed within the National Institute of Health and Welfare, and has a mandate to collect and collate health and social data from relevant registries and combine various data sets for its customers. Findata also anonymize information prior to disclosure for secondary purposes. For example, for access for innovation and development purposes, it is possible to specifically request Findata to collect and combine personal data from several different registries. After accepting the request, Findata will process the data and provide a set of aggregated, statistical data to the requesting party.

In general, health and social data is accessible through a data permit application or a data request, dependent on the required information and purpose of use. Primarily, data provided by Findata is delivered in a secure online environment. The nature and form of the data depends on the purpose of use stated in the data permit or data request.

For access for secondary use purposes, the Finnish regulations provide legal basis for combining health and social data, establishing secure user environments and user interfaces for supply of data, as well easy access to health and social data.

The objective of this section covering Finland is to explain legislation enabling secondary use of health and social data, and to provide a brief introduction on available information resources, processes and key authorities. Following this general overview, access to health and social data for specific secondary use purposes under relevant legislation will be elaborated on. In this regard, focus will be on secondary use for innovation and development purposes.

8.2 Finnish social and health care system and information resources

In Finland, the state's responsibility to promote welfare, health and security is stated in the Constitution of Finland. The Finnish social and health care system is based on municipal social welfare and health care services and is established with support from the government.

Finland has comprehensive high-quality information resources in the field of social and health care.

Public and private service providers operate alongside each other, and several governmental agencies and organizations participate in developing, maintaining and providing information management to the system.

Over the past decades, Finland has developed comprehensive and high-quality information resources in the field of social and health care. For years, these information resources have been utilized for scientific research and statistics. The legal landscape also acknowledges other secondary use purposes, hereunder innovation and development.

In general, service providers keep health and social data registries in electronic form, and Finland has a long tradition of developing digital services for the social welfare and health care sector, which benefit the citizens, as well as social welfare and health care service providers.

The Finnish Kanta services[325] is a prime example of the maturity and scale of the Finnish health and social data digital services. Kanta services are maintained by the Social Insurance Institution of Finland (Kela), which is a governmental agency that provides basic economic security for everyone living in Finland.

[324] Findata, https://www.findata.fi/

[325] Kanta, https://www.kanta.fi/en/. According to Kanta statistics as of 31.12.2019, the number of documents on service transactions and treatment (all versions) restored in the Patient Data Repository was 1 784 158 170,

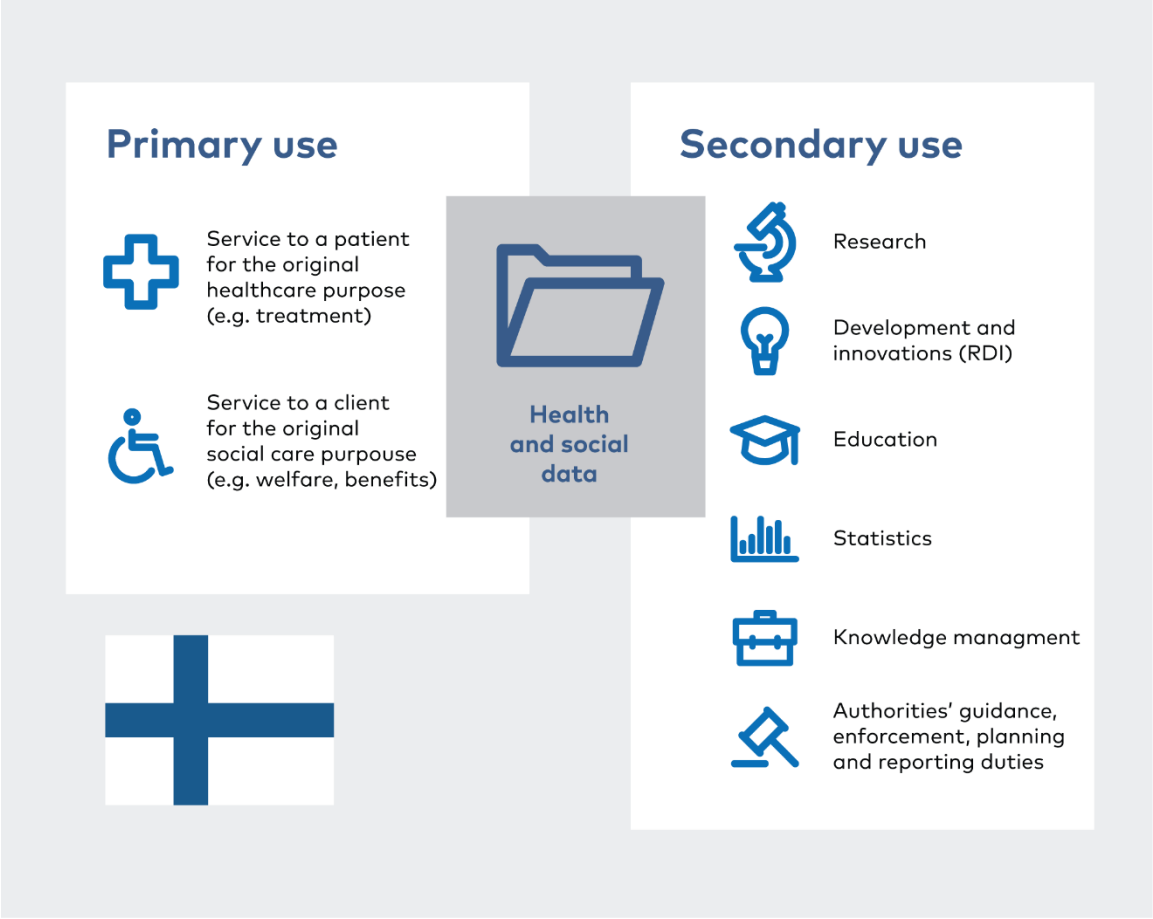


Figure 6 - Regulated division of primary and secondary use of health and social data in Finland

Kanta services include a national Patient Data Repository, which allows centralized electronic archiving of medical records and long-term storage of the data. Health care professionals register patient data in the Patient Data Repository and update the medical records with any information necessary for the treatment. Medical records are also updated upon each service event. Medical records are generally preserved for 12 years after a person's death.

Kanta services are extended to also provide Client Data Archive for Social Welfare Services. This nationwide information system enables centralized electronic archiving of social welfare client data, as well as active use and permanent storage of the data.[326] Further, as a principal rule, all prescriptions must be issued electronically.[327] Prescriptions are saved in the Prescription Centre, the centralized database for prescription data in the Kanta service. Health care professionals and pharmacies, that have joined the electronic prescription service pursuant to the conditions provided by law, access the information through medical records or pharmacy systems.

There is a significant number of major Finnish sources for health and social data, besides the public and private sector health and social services providers. Other important health and social data operators and information resources that are regulated by law are the National Institute for Health and Welfare, Social Insurance Institution of Finland, Finnish Centre for Pensions, the Statistics Finland, National Supervisory Authority for Welfare and Health (Valvira), the Finnish Medicines Agency (Fimea), Finnish Institute of

Finland is one of the pioneers in Europe in enabling effective and secure access to health and social data.

[326] Kanta, https://www.kanta.fi/en/professionals/client-data-archive-for-social-welfare-services

[327] Kanta, https://www.kanta.fi/en/professionals/prescription

Occupational Health and Digital and Populations Data Agency.

8.3 General principles on use of health and social data

8.3.1 General

As in the other countries and self governing territories in the Nordic region, processing of health and social care data is strictly regulated under Finish law.[328] Health and social data form a special category of data, which is sensitive in nature. Such data is not only subject to professional secrecy and confidentiality obligations but can also only be used for the primary purpose the data originally was collected for.

As an example, in the Act on the Status and Rights of Patients of 17 August 1992 section 13, it is stated that information contained in medical records is confidential and as a principal rule cannot be disclosed to a third party without the patient's written consent. Primary use of health data is used to assess, restore or maintain a person's health performed by the health care unit where the data was collected, or provide treatment to the patient in question.

When providing health and social care, professionals must not disclose the information to third parties without the patient's or social care client's explicit written consent, except in special circumstances regulated by the law.

Consequently, in Finland, processing health and social data for secondary uses requires authorization.

With the Finnish legal reform and introduction of the Finnish Act on the Secondary Use of Health and Social Data, the new regulatory authority Findata was granted a regulatory mandate, which provides Findata with a legal basis to process the data for preparatory purposes, including anonymization. Findata is authorized and obligated for example to aggregate social and health data into a state that satisfies the legal requirements for confidentiality and data privacy.

8.3.2 Available data materials

Findata's operations, role and responsibilities are regulated by the Act on the Secondary Use of Health and Social Data. Findata's objective is to promote secondary use of social and health data, reduce the permission period for access to data, and improve data protection. Findata provides services where data from several data controllers is requested, where data is collected from private social welfare or health care service providers, and where data is stored in Kanta services.

The following data materials are available from Findata for secondary use.[329]

- Aggregated data / statistical data: This type of data is available for, *inter alia*, development and innovations purposes. Aggregation is a statistical procedure that combines data and creates combinations of several separate data elements. Aggregated information indicates that the information concerns a group of persons instead of a specific person. In practice, the process involves anonymization of data, as the aggregated information is structured so that individuals cannot be identified. In statistical data, individual personal data has been combined and summarized. As with aggregated data, such data is regarded anonymized data. As anonymized data is not regarded personal data, the requirements set forth in the GDPR are not applicable. Anonymized data may be subject to cross-border transfers and processing of such data is not restricted by privacy regulation.
- Personal / customer data: This type of data is confidential personal data covered by the GDPR and national legislation. Data is stored in a customer registers or in an associated administrative registry for social and health care customer relationship or for processing of benefits. Pseudonymized Personal / customer health and social care data is also accessible on a data permit basis, e.g. scientific research or statistics purposes, but not for development and innovation purposes. There are certain preconditions for receiving such data permit, such as use of scientific methods, as regulated by the GDPR and the Finnish Data Protection Act of 5 December 2018.

Findata services are subject to service fees and specified services and materials are in principle available outside the EEA, including to data permit holders operating outside these regions.[330]

> *Use of health and social data is strictly regulated in Finland due to the sensitive and confidential nature of these data.*

[328] The processing of personal data covers all processing activities involving personal data, from the planning of processing to the collection, storage, use, transfer, disclosure and erasure of personal data.
[329] In the event there is only one data controller for the required data, related data permit or data request is handled and granted by the data controller. However, any required aggregation of the data is always conducted by Findata.
[330] Findata services have had limitations in connection with commencement of the service provision, as data requests have been possible only with a Finnish personal identity code through Suomi.fi identification. Findata has mapped alternative secure identification applications for international clients.

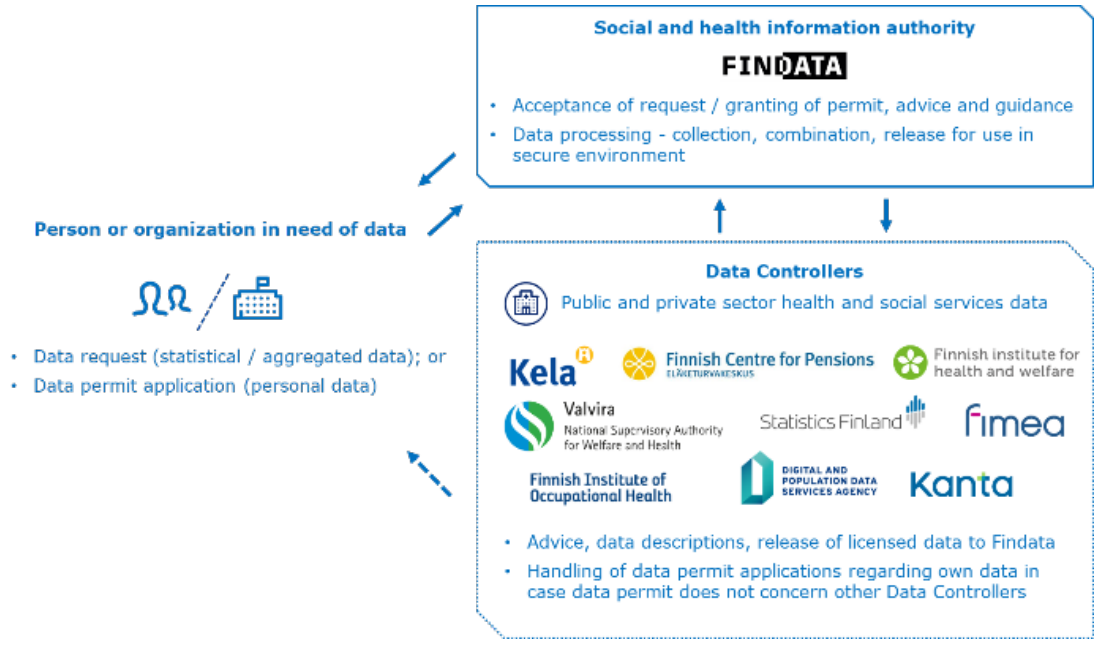


Figure 7 - The Finnish process for acquiring health and social data for secondary use

8.4 Legislation

8.4.1 General

Prior to the Act on the Secondary Use of Health and Social Data, secondary use was regulated by individual sections in several different acts, covering mainly historical or scientific research and statistics use. No legislation addressed use of health and social data for development and innovation purposes.

By enacting the Act on the Secondary Use of Health and Social Data, the legislator streamlined the legal landscape. The individual sections regarding secondary use were repealed and regulation regarding secondary use of social and health data were centralized to a single act. Around the same time, the Finnish Personal Data Act from 1991 was repealed and replaced by the Finnish Data Protection Act of 5 December 2018, with the objective of specifying and supplementing the articles of the GDPR.

The Act on the Secondary Use of Health and Social Data contains detailed sections including e.g. purposes for which data can be obtained, justifications and conditions for the secondary use, as well as applicable processes for obtaining access to data materials and supervision organization. The Finnish Data Protection Act addresses processing of personal data on a more general level. As part of the legal reform, the Act on the National Institute for Health and Welfare of 31 October 2008 was amended, and the tasks and duties of the National Institute for Health and Welfare were redefined and aligned with the Act on the Secondary Use of Health and Social Data.

In addition to the Act on the Secondary Use of Health and Social Data, the Statistics Act of 23 April 2004 regulates use of data for scientific research when data used in the research has been collected for statistical purposes from Statistics Finland or the National Institute for Health and Welfare (the Statistical Authorities). The Statistical Authorities will be covered in more detail below.

In 2020, other legal reforms relating to the GDPR regarding the field of medical research are in progress. A government proposal for a new Biobank Act, repealing the act from 2012, is under preparation. The purpose of the new act is to further improve biobank-related research by automatically allowing use of hospital-based biological samples collected upon treatment, unless the individual refuses such use. Further, the objective is to align the new act with the GDPR and the Act on the Secondary Use of Health and Social Data. The government bill includes a provision for obtaining biobank data for development and innovation purposes, provided that an explicit consent from the sample donor is obtained, and that authorization by the Data Permit Authority (Findata) is granted.[331] At the time of this report, it is estimated that the government bill on the new Biobank Act will be presented to the Parliament of Finland by the end of May 2020.

[331] Government bill on the new Biobank Act, p.1. Available online in Finnish: https://api.hankeikkuna.fi/asiakirjat/3834550f-ae72-42b7-b227-030639631b9a/1c7533e8-9471-429d-833b-1f436d7907f0/MUISTIO_20180406070553.pdf

In addition, the new Genome Act has been prepared. The purpose of the Act is to support responsible, equal and secure use of genomic data for the benefit of human health. The objectives, *inter alia*, are to create a genome registry for genetic ancestry of the Finnish population, with the intention to use the same genetic ancestry e.g. for the prevention of national diseases. In addition, a National Genome Center is proposed established, intended to serve as a center of excellence for processing and storage of data to enable its utilization. Throughout the opinion rounds, the initial draft for the new Genome Act raised discussions on gathering on highly sensitive personal data, and, at the time this report, the draft for the Act is under further preparation. The Ministry of Social Affairs and Health has informed that the draft is being modified based on the received feedback. The new draft of the Genome Act was planned to be presented to the Parliament of Finland at the same time as the new Biobank Act, by the end of May 2020.

8.4.2 The Act on Secondary Use of Health and Social Data

The Act on Secondary Use of Health and Social Data came into force on 1 May 2019. Secondary use of health and social data means that data created during the provision of health and social care can be used for other than the primary use purposes they originally were collected for. Health and social data for secondary use is available from the following registries and sources:

1. Data saved in Kanta services, which will be available from 2021;
2. Data from social and health care providers (public and private sector);
3. Data on social benefits from the Social Insurance Institution of Finland (Kela) and the Finnish Centre for Pensions (Eläketurvakeskus);
4. National registries and survey materials from National Institute for Health and Welfare, Social Insurance Institution of Finland, Finnish Centre for Pensions and the Statistics Finland's register on causes of death;
5. Information on health and social services from Valvira, the Finnish Institute for Occupational health (Työterveyslaitos) and the regional state administrative agencies; and
6. Basic information on persons and buildings from the Population Register Centre, for purposes regulated by law.[332]

According to the Act on Secondary Use of Health and Social Data section 6, the responsibility for producing the secondary use services lies with the Data Permit Authority Findata, and the following authorities and organizations:

1. Ministry of Social Affairs and Health;
2. National Institute for Health and Welfare, notwithstanding data collected for statistical purposes as a statistical authority;
3. Social Insurance Institution of Finland, insofar as the data needed for the purposes stated in the Act is personal data stored during processing of benefits in a customer relationship, or concerns drug prescriptions and associated delivery information stored in a prescription center referred to in the Act on Electronic Prescriptions (61/2007) section 3, paragraph 4, and in a prescription archive referred to in paragraph 5;
4. National Supervisory Authority for Welfare and Health Valvira;
5. Regional State Administrative Agencies, insofar as they process matters related to social and health care;
6. Finnish Institute of Occupational Health, insofar as the data needed for the purposes stated in this Act comes from occupational disease registers and exposure measurement registers and the Institute's patient registers;
7. Finnish Medicines Agency Fimea;
8. Public service organizers of social and health care;
9. Statistics Finland insofar, as the data needed for the purposes stated in this Act is data referred to in the Act on Determining the Cause of Death (459/1973);
10. Finnish Centre for Pensions, insofar as the data needed for the purposes stated in this Act is necessary personal data stored in the Finnish Centre for Pensions' registers, and concerns employment and earnings information stored during the implementation of earnings-related pension, granted benefits and their justifications, including disability pension diagnoses; and
11. Population Register Centre, insofar as the data needed for the purposes stated in this Act comes from the Population Information System and is basic data on individuals, their family relationships and places of residence, as well as data on buildings.

In general, and for most of the secondary purposes, such as development and innovation, access to data is anonymized either by aggregation, or in a way that the data subject is not identifiable, directly or indirectly. In addition, data necessary for the defined purpose is made accessible only to a minimum extent. In specific cases, data containing identifiers is available, provided that the procedures in the Act are followed.

[332] For further reading, please refer to: https://stm.fi/en/secondary-use-of-health-and-social-data

According to the Act on Secondary Use of Health and Social Data section 2 (Scope of application), data created for primary use can be used for the following secondary use purposes:

- statistics
- scientific research
- development and innovation activities
- steering and supervision of authorities
- planning and reporting duties by authorities
- teaching
- knowledge management

The government bill for the Act on Secondary Use of Health and Social Data defines development and innovation activities as application and use of technical, business and other existing information together with health and social data for the development of new or significantly improved products, processes or services. 333

The Act on Secondary Use of Health and Social Data harmonizes data access and the authorization process. Authorization is granted by Findata when data is required from various controllers, when data is required from private health and social services, or when the data request relate to data saved to the Kanta Services. If data from a single controller is needed, that controller may grant the data permit for secondary use. Controllers, together with Findata, can also decide that the authority shall handle the task on behalf of the controller.

Anyone requiring Finnish health or social data for the secondary use purposes listed above can submit a data request or apply for a data permit to the data authority Findata.

8.4.3 Data permit authority Findata

As mentioned above, Findata started its operations in 2020. It operates in conjunction with the Finnish Institute for Health and Welfare but are separated from the Institute's other activities. The operations are supervised by the Parliamentary Ombudsman of Finland and the Office of the Data Protection Ombudsman, while The Ministry of Social Affairs and Health provides Findata with performance guidance.

When data is requested from more than one data controllers, Findata serves as a single point of contact for access to secondary use of health and social data. Several tasks have been centralized and assigned to Findata in accordance with the Act on the Secondary Use of Health and Social Data, the most essential being evaluating data requests and granting data permits, which are two separate activities concerning different applications, collecting and combining data, providing a secured environment for processing of data, as well as supervising data permit holders. Findata also offers an advisory service for its customers.

Findata is entitled to obtain and process data without regarding professional secrecy obligations when carrying out its assigned tasks.[334] Findata has the right to obtain the following information from the controllers:

- Information required to grant a data permit;
- Data referred to in a granted data permit to collect, combine and pre-process and disclose data for processing to the data permit holder;
- Information required to assess whether the data referred to in the data permit application can be anonymized or whether aggregated statistics can be produced from data referred to in the Act on Secondary Use of Health and Social Data section 45;
- Data required to generate aggregated statistics; and
- Data required to collect the pre-processed data sets referred to in The Act on Secondary Use of Health and Social Data section 14.5.

Findata's objective is to facilitate for use of valuable health and social data for worthy causes, such as for development of more effective medicines, and increase information supply for research purposes.

8.4.4 The National Institute for Health and Welfare and Statistics Finland

The National Institute for Health and Welfare (THL) is an independent agency operating under the Ministry of Social Affairs and Health.[335] In connection with the legal reform, the tasks of the National Institute for Health and Welfare were redefined and aligned with the Act on Secondary Use of Health and Social Data.

Regulated responsibilities include studying and monitoring the welfare and health of the population, assessing factors affecting and problems related to the welfare and health of the population, prevalence of these problems, and opportunities for prevention. The institute develops and promotes measures to further improve welfare and health, as well as to reduce welfare and health problems. A new task aligned with the Act on Secondary Use of Health and Social Data responsibility is to promote development and innovation activities within the field of social and health care, where the National Institute for

[333] Government proposal on the Act on the Secondary Use of Health and Social Data and thereto related legislation 159/2017, p.91.

[334] The Act on the Secondary Use of Health and Social Data section 36

[335] THL, https://thl.fi/en/web/thlfi-en/about-us/what-is-thl-

Health and Welfare hold wide-ranging statistics and registries.[336]

Statistics Finland is the only Finnish public authority specifically established for statistics purposes and produce most of the Finnish official statistics.[337] Statistics Finland produces approximately 160 sets of statistics on a wide range of topics each year. All statistics are released on their webpages. Among these statistics are 17 sets of health statistics, including statistics on e.g. alcoholic beverage consumption and causes of death.

According to the Statistics Act of 23 April 2004, and as an exception from the general responsibilities of Findata, when required data relates to data collected by the Statistics Finland or the National Institute for Health and Welfare, these statistical authorities are responsible for granting data permits for scientific research, and for combining the data associated with the research plan to their own data. In addition, in these cases, they are responsible for the pseudonymization or anonymization of the data. According to the Act, the information can be disclosed for scientific research purposes only, and solely in a manner where statistic units can be identified indirectly only. The basis for this exception is that information collected for statistical purposes is to be covered by statistical confidentiality.

According to the Statistics Act section 13, classified information obtained for statistical purposes can be disclosed to third parties only on the grounds set out in a law applicable to state statistical authorities or be based on the consent of the data subject. It is prohibited to disclose classified information for administrative decision-making or similar processing purposes. According to the section, the statistical authority may disclose classified information it has collected for e.g. statistical purposes for scientific research and statistical studies related to social conditions. Although disclosure of personal data and other identifiable data on statistical objects is generally prohibited, the statistical authority can grant access to such classified data where a statistical object can be identified indirectly.

The processing of data collected for statistical purposes is governed by the GDPR, the Data Protection Act of 5 December 2018 and the Act on the Openness of Government Activities of 21 May 1991, unless otherwise provided by Statistics Act or another law.

8.4.5 Social and health Data for development and innovation purposes

According to the Act on Secondary Use of Health and Social Data, health and social data can be obtained for development and innovation purposes only in the form of anonymized aggregated statistics.[338] The data is anonymized by Findata.

Aggregated statistics refers to reliably produced anonymized data in a statistical form.[339] Aggregation is viewed as a necessity because anonymizing data simply by deleting names, addresses and other direct identifiers not necessarily is sufficient, as information that allow for the individual to be indirectly identified must also be deleted. This information may include, for example, information on rare diseases or specific social welfare benefits. Anonymized data is no longer regarded as personal data and, therefore, no longer subject to the articles of the GDPR.

In Finland, the concept of development and innovation is intended to extend the opportunities to utilize health and social data beyond the traditional scientific research. Definitions of development and innovation activities are explained in the government bill for the Act on Secondary Use of Health and Social Data. The definitions refer to a new product, service or activity that generates economic or social benefits.[340] Innovation is also to be interpreted as a broader concept than research and development, and product or process innovations can include marketing and organizational innovations that are deployed within the organization.[341] Development activities refer to experimental development activities carried out by various systematic methods in research organizations, companies and public organizations for scientific, technical and commercial purposes by using relevant knowledge and skills to develop plans or models for new, modified or improved products, processes and services.[342]

Further, it is notable that the use of personal data for the purposes of development and innovation activities would not require the activities to be carried out in accordance with scientific research methods, since such development and innovation activities would be subject to scientific research provisions. The provisions and specific conditions to conduct scientific or historic research are in the Finnish Data Protection Act, according to which such processing is based on an appropriate research plan, the research has a responsible person or a group responsible for it, personal data will be used (processed) and disclosed only for historical or scientific research or other compatible purposes, and personal data of specific individuals will not be disclosed to third parties. Having only anonymized,

[336] Overview THL's statistics and registers, https://thl.fi/en/web/thlfi-en/statistics/statistics-by-topic
[337] Statistics Finland, https://www.stat.fi/org/index_en.html
[338] The Act on the Secondary Use of Health and Social Data section 37.
[339] Ibid. section 1 (18).
[340] Ibid. section 37.
[341] Government proposal on the Act on the Secondary Use of Health and Social Data and thereto related legislation 159/2017, p.125.
[342] Ibid p.126.

aggregated statistics for innovation and development purposes was not the original plan in Finland. The initial preparation for the Act included an option that social and health data could be obtained for development and innovation purposes also based on a data subjects consent pursuant to a data permit. In that case, the data would have been identifiable personal data instead of anonymized data.

However, consent option was not included in the Act after the Parliament of Finland's Committee for Constitutional Law (perustuslakivaliokunta) raised its concerns, considering that it is evident that disclosure of social and health data for development and innovation purposes cannot be based, for example, on a consent given during provision of social welfare related administrative procedures or provision of health care services. In the Committee's view, a consent given under these unbalanced circumstances is not truly voluntary and the social care customer or patient has not necessarily the opportunity to consider the meaning and importance of the consent.[343] In addition, the Committee feared that the consent option introduced by the Act could enable use of sensitive social and health data with large-scale commercial purposes.[344] Thus, the Act ended up to provide that the only available data for development and innovation purposes is aggregated statistical data.

Findata is entitled to generate aggregated statistical data based on a data request. However, there are specific conditions for disclosing the requested data.[345] The data request, with the data utilization plan enclosed, must state that the purpose of development, and that the innovation activity is to:

- promote public health or social security;
- develop social and health care services or service system; or
- protect the health or wellbeing of individuals or secure their rights and liberties associated with their health or wellbeing.

When assessing the data request, Findata must consider whether it is possible to generate the aggregated statistical data from the registry information submitted by the requestor.[346] This assessment must be based on the GDPR Article 9 (2g) and Article 86**.** Findata must also consider the guidelines of the expert group referred to in the Act on Secondary Use of Health and Social Data.[347]

As introduced above, aggregated statistical data is not regarded as personal data. Thus, a legal basis for processing in accordance with the GDPR Article 6 is not required.[348] Consequently, the process for obtaining the same data can be based on a data request instead of a data permit application.

Based on data request, aggregated statistical data is also available for all other secondary use purposes listed in the Act on Secondary Use of Health and Social Data.

8.4.6 Data disclosed pursuant to a data permit

In addition to access to anonymized aggregated statistics data described above, which is available for e.g. innovation and development purposes, in specific cases, personal data *as such* is required for other purposes.

Health and social data can be disclosed pursuant to a data permit for scientific research and statistics, education, and for the planning and reporting duty of the government.[349] A permit can only be granted if it is evident that providing the personal data in question does not violate the interests for those protected by the duty to professional secrecy.[350]

Data in registries with public controllers or in registries of private social or health care service providers, may be processed for secondary use under a temporary data permit issued either by the relevant controller, Findata or otherwise pursuant to the Act on Secondary Use of Health and Social Data.[351] The basis for processing is derived from the GDPR the Article 6 and Article 9 regarding special categories of personal data, such as health data and genetic data.

8.4.7 Scientific research

Scientific research is one of the listed secondary use purposes requiring a data permit.[352] In individual cases, notwithstanding professional secrecy obligations, Findata may grant a data permit to access personal data held by organizations referred to in section 6 of the Act.[353] Freedom of scientific research must be ensured when procuring a data permit.

The GDPR recognize the value of personal data being processed for scientific research purposes and register

[343] Opinion of the Committee for Constitutional Law PeVL 1/2018, p.10. Available online: https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_1+2018.aspx
[344] Ibid. p.6.
[345] Subject to processing of data request pursuant to the Act on the Secondary Use of Health and Social Data section 45.
[346] In accordance with the Act on the Secondary Use of Health and Social Data section 45.
[347] Guidelines of the reference group are referred to in the Act on the Secondary Use of Health and Social Data section 8 (4).
[348] Government proposal on the Act on the Secondary Use of Health and Social Data and thereto related legislation 159/2017, p.125
[349] The Act on the Secondary Use of Health and Social Data sections 38, 39 and 40.
[350] P. 6 in the Frequently asked questions about the Act on the Secondary Use of Health and Personal Data-Pdf.
[351] The Act on the Secondary Use of Health and Social Data section 35, addressing the general justifications for secondary use.
[352] For example, innovation and research do not fall under data permits, but data requests, as explained above.
[353] The Act on the Secondary Use of Health and Social Data section 38.

studies.[354] According to Article 5 (1b) of the GDPR, scientific research and statistics are not considered incompatible with the primary purposes for use for personal data.

In addition, when data is processed for scientific research and statistics, the processing of data for scientific research and statistics regulation in the Data Protection Act applies. The Data Protection Act includes sections on processing of personal identity codes, in addition to derogations and safeguards on processing of personal data for scientific and historical research and statistical purposes.[355]

8.4.8 General requirements for granting a data permit

When personal data is required, instead of anonymized aggregated statistics data and a related data request, a data permit for the secondary use of personal data may be granted to an applicant provided that all general requirements are fulfilled.[356]

Firstly, a data permit may be granted if the intended data purpose stated in the application and the data utilization plan enclosed conform the articles of the GDPR, The Data Protection Act, the Act on Secondary Use of Health and Social Data, as well as any other applicable act, and if the intended purpose is most appropriately achieved by using the information referred to in the application.[357] Thus, the information requested in the application must be proportionate to the purpose pursued. Personal data required must be appropriate and relevant to the purpose and limited to what is necessary for processing purposes.[358] The principle of data minimization referred in the GDPR has thus been considered.[359]

Secondly, ff the data permit application includes an intended purpose for which separate provisions regulated the application procedure and the permit grounds, all additional requirements must be met.[360]

Thirdly, if the data to be disclosed have been collected with the data subject's consent, a data permit for data concerning the data subject may be granted only if the disclosure and use of the data conforms the terms and conditions of the consent.[361]. The purpose of this rule is to safeguard the sovereignty of the individual.

The Act on Secondary Use of Health and Social Data essentially corresponds with section 28 of the Act on the Openness of Government Activities and addresses the term of the data permit and protecting the interests of the data subject.[362] A data permit may be given for a fixed period of time if it is undoubtedly that disclosure of the data does not infringe the interests safeguarded by the professional secrecy obligation.[363] Findata is responsible for evaluating and determine whether the legal requirements are fulfilled, including the data applicant's ability to protect the data.

Findata is also responsible for verifying that the use of the data is compliant with the existing legislation. The assessment is based on a broader legal framework, particularly ensuring that the processing of the data complies with the articles of the GDPR.[364] The permit consideration also involves the consideration of expediency (*in Finnish: tarkoituksenmukaisuusharkinta*). In cases where the data permit application is denied due to expediency, it should be justified objectively. A permit can also be withdrawn if considered appropriate. If a data permit application is withdrawn after it is granted, this shall be based on a formal decision of Findata, which may be appealed by the applicant.[365]

Lastly, if Findata consider that a data permit application instead should be processed as a data request pursuant to section 45 of the Act, Findata shall contact the applicant and propose that the matter should be processed as a data request.[366] If the applicant insists that the matter is handled as a data permit application, Findata must make a decision. If the applicant agrees to handle the matter as a data request or does not respond within the deadline set by Findata, Findata may handle the matter as a data request.[367]

8.4.9 Applying for a data permit or submitting a data request

As described above, when data is required for a legitimate secondary use purpose, either a data request or a data permit application may be submitted to Findata. The purpose of use and nature of the data determines if the data can be obtained pursuant to a data request or if a data permit is required.

The data request or data permit application must be submitted to Findata via an electronic data request management system.[368] Data requests and data permit applications must be submitted together with a data

[354] The GDPR recitals 157 and 159.
[355] The Finnish Data Protection Act sections 4,6,29 and 31, https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf
[356] Data permit requirements are listed in the Act on the Secondary Use of Health and Social Data section 43.
[357] Ibid. section 43 (1).
[358] Government proposal on the Act on the Secondary Use of Health and Social Data and thereto related legislation 159/2017 p.37.
[359] The GDPR Article 5 (1) c)
[360] The Act on the Secondary Use of Health and Social Data section 43 (2).
[361] L.c.
[362] The Act on the Secondary Use of Health and Social Data section 43 (4).
[363] L.c.
[364] Government proposal on the Act on the Secondary Use of Health and Social Data and thereto related legislation 159/2017 p.138.
[365] The Act on the Secondary Use of Health and Social Data section 58 (5).
[366] Ibid. 43 (5).
[367] Government proposal on the Act on the Secondary Use of Health and Social Data and thereto related legislation 159/2017 p.138.
[368] As referred to in the Act on the Secondary Use of Health and Social Data section 16.

utilization plan. Requirements for the data utilization plan is described in the Act.[369] Accordingly, a data utilization plan refers to a research plan, project plan or similar plan stating the intended purpose of the requested data, the controller and processors for the data, the legal basis for processing, as well as data security and data protection related to processing throughout the lifecycle of the data, including storage, erasure and archiving. If the applicant is asked to supplement their application, any supplement must be submitted via the data request management system. The data permit decision will be notified the applicant via the same system. Findata may also issue detailed provisions for data permit applications, data utilization plans, and the data requests using the system.[370]

The data request management system can be accessed on Findata's website.[371] Findata started receiving data requests via the data request management system on 1 January 2020, and data permit applications as of 1 April 2020.[372] Services are available only with a Finnish personal identity code via the Suomi.fi identification method.[373] At the time of this report, Findata is in the process of mapping alternative secure identification methods for other clients.

After submission, Findata examines and processes the data request or data permit application. The decision shall include all necessary information, and must be provided without undue delay, and no later than 3 months after the complete application is received by Findata. Findata can prolong providing the final decision with an additional period of 3 months due to e.g. the challenging nature of the case.

Findata contacts concerned data controllers on the basis of an accepted data request or data permit application. The data controllers must disclose the data referred upon the request by Findata without undue delay.[374] The data disclosure shall, in any case, be made within 30 working days from the date Findata made a favorable decision on disclosing the data to the applicant. Findata shall inform the applicant required clarifications without delay, after which the requested data must be submitted within 30 working days from the reception of additional clarification, if the clarifications enable Findata to verify that the requirements for data disclosure are met. In cases where the controller is unable to disclose the data to Findata within the deadline, the controller must report the delay, its cause, and any deadline extension needed before the initial deadline has expired. Based on a valid reason, Findata will set a new deadline.

Findata must disclose data to a permit holder without delay and no later than within 60 working days from granting the permit. For compelling reasons, Findata may extend the deadline, provided that the data requires exceptionally extensive processing of data from several controllers, or a particularly challenging combination process. Findata must inform the permit holder of the extension, the justification for the extension and the new deadline for when the data will be disclosed.

8.5 Transfer of and transborder access to social and health data

In terms of accessing Finnish health and social data, the Act on the Secondary Use of Health and Social Data provides the same opportunities to Finnish nationals, as to foreigners. This also applies for access for innovation and development purposes.

In addition to the GDPR articles, there are sections in the Act on the Secondary Use of Health and Social Data explicitly regulating transfer of data obtained for a lawful secondary use purpose.[375]

As a rule, health and social data can only be processed in a centralized secure user environment maintained by the data permit authority Findata. Use of the secure environment requires granted access rights in form of a data permit. Only in exceptional circumstances can the data be provided to other secure user environments specified by the data permit holder.[376]

In addition to the secure user environment requirement, personal data obtained pursuant to a data permit may only be used for the purpose for which it has been granted. Data cannot be disclosed to others than the recipient of the data permit.

As aggregated / statistical data is not considered as personal information, the GDPR do not apply. Thus, such data can be transferred regardless of the abovementioned conditions. This also applies for access for innovation and development purposes.

Health and social data for secondary use is processed in Findata's secure user environment.

[369] The Act on the Secondary Use of Health and Social Data section 3 (17).
[370] Ibid. section 46 (2).
[371] Findata, https://lupa.findata.csc.fi/
[372] Findata, https://www.findata.fi/en/services/
[373] Ibid.
[374] The Act on the Secondary Use of Health and Social Data section 48.
[375] The Finnish Act on the Secondary Use of Health and Social Data section 20.
[376] In this case, the secure user environment specified by the permit holder must meet the secure operating environment conditions set out in sections 21-29 of the act.

8.6 National obstacles

8.6.1 Specific regulation for the secondary use of health and social data

In Finland, the Act on Secondary Use of Health and Social Data, together with supplementing regulation, provides specific opportunities for collation of health and social data for secondary use purposes.

Although secondary use of health and social data previously has been possible for historical or scientific research and statistics purposes, the new Act provides a wider range of alternative secondary use purposes, including innovation and non-scientific research.

In addition, a centralized system for collection and administration of information requests pertaining to multiple controllers of health and social data significantly benefit all interested parties. Authority Findata's role as the first point of contact when data is required from multiple controllers is likely to enhance the process of collecting and obtaining data, lowering future administrative burden and cost.

8.6.2 Accessible data for development and innovation purposes is aggregated

One of the initial objectives emphasized by the Finnish legislator preparation of the Act on Secondary Use of Health and Social Data was to facilitate for use of personal data for development and innovation purposes, extending the opportunities beyond scientific research and statistics purposes.

Although this objective is met, the circumstances in which access can be obtained to social and health data for development and innovation activities remain limited due to weighty, fundamental reasons related to data subject rights. Health and social data can only be obtained in form of aggregated statistics for development and innovation purposes, which to some extent may limit the variability and usability of available data.

8.6.3 Practical obstacles for foreign clients

At the time of this report, another obstacle that affect foreign clients especially, is that data requests are only possible to submit with a Finnish personal identity code via the Suomi.fi identification portal, which limits the possibilities for data access for foreign clients. However, Findata is mapping alternative secure identification applications for those not possessing a Finnish personal identity code.

9. Åland

Åland Islands, or Åland, is an self-governing autonomous archipelago province at the entrance to the Gulf of Bothnia in the Baltic Sea belonging to. Åland's autonomy is based on section 1 of the Act on the Autonomy of Åland of 16 August 1991. The Parliament of Åland represents the people of Åland in matters relating to its autonomy, whereas the Governor of Åland represents the Government of Finland.

The Parliament of Åland passes acts in areas relating to the internal affairs of the region and exercises its own budgetary power. Matters relating to patient rights and data protection are regulated by the applicable Finnish legislation and the Act on Secondary Use of Health and Social Data is applicable in its entirety in Åland. The available information resources, processes and key authorities, such as Findata, are equally relevant for Åland as they are for the rest of the Finland.

Åland's Landskapslag om hälso- och sjukvård (2011:114) regulates the public health care in the province and includes general provisions on e.g. what kind of care is offered and how the care is organized and supervised.[377]

The GDPR is applicable in Åland, and Åland has its own data protection authority, Datainspektionen.[378]

[377] Available online in Swedish: https://www.regeringen.ax/alandsk-lagstiftning/alex/2011114#pr_3_kap_de_grundlaggande_bestammelserna_om_clands_halso-_och_sjukvards_verksamhet_16_p
378 Datainspektionen, https://www.di.ax/om-oss

10. Iceland

10.1 Introduction

Icelandic health data is considered a significant data resource. As the emigration rate is low, health data exist for most citizens throughout their lifetime. Health data has been collected for a long period of time, and electronic health data reaches back to the 1980s.[379]

Individuals' health data are collected in connection with provision of health care at several health care facilities, such as hospitals, health care centers, private practices[380] and nursing homes. Thus, information is stored with different data controllers. For this reason, it is important that the national infrastructure and legal environment enables the possibility to interconnect individuals' health data from various data sources. By doing so, it is possible to integrate information and enhance efficient coordination among health care providers for the purpose of providing individuals the best health services possible. Health data sets are also considered a valuable source for innovation and development, as well as for scientific research. Iceland has succeeded in modernizing and digitalizing its health care systems and measures are constantly taken for further development and to obtain a more effective and innovative health sector. Compared to other countries, Iceland has advanced by building a nationwide uniform medical record system. At the time of this report, Iceland is considered to have a reliable public health data infrastructure, which enables integration of individuals' health data from multiple sources using ID numbering. Although medical records are interconnected, the Icelandic system is decentralized and there is no centralized entity providing a shared entrance to all health data, neither from medical records nor other sources, for secondary use purposes. For access to health data, each relevant data controller must be approached and a request for access must be submitted.

Icelandic legislation focusses on enabling secondary use of health data for scientific research, as well as for other limited purposes. Iceland has several legal frameworks specifically on processing of health data in accordance with the Data Protection requirements, allowing processing of health data for various reasons of substantial public interest. Processing of health data for innovation and development activities is generally not permitted under the framework and access to health data for innovation activities is only regulated in a holistic manner.

The legislation focuses on enabling secondary use of health data for scientific research.

Processing of health data for innovation and development activities in general is not covered.

10.2 Icelandic health care system and information resources

10.2.1 General

The health care system is a cornerstone of Icelandic society. The system is mostly publicly funded, and the underlying principle is that the state guarantees necessary health services, irrespective of the individual financial standing or other circumstances. The Minister of Health (MoH) is the director of health affairs in Iceland. The health care institutions, ministers, and other bodies under the MoH play a vital role in the health sector, as the health system is integrated and connected with all aspects of society. Private service providers operate alongside the public sector and several governmental agencies and organizations have supportive roles within the system. The Health Services Act[381] lay down the structure of national health services, the objective being to provide Icelanders with access to the best health care possible provided at any time.

Iceland has comprehensive and high-quality information resources within the health sector. Health data is stored in medical records, biobanks and health registries, as well as in mandatory public archives, quality registries, and in Statistics Iceland's databases.

All health care providers are obligated to keep medical records in an electronic form to the extent possible.[382] As digitalization hold an important role in reforming health care in Iceland, steady progress for increasing information technology within the health care system has been made. Although the health care system is decentralized, there is an option of interconnecting health information systems to ensure access to patient information.[383] However, as it is voluntary to participate in the interconnected system, it is difficult to ensure that the system is fully interoperable. Effort has been made by the DoH to make all health care providers to participate. At the time of this report, all public and most private health care providers within the

[379] Electronic Causes of Death Register began 1971 and electronic Birth Register began 1972: https://www.landlaeknir.is/tolfraedi-og-rannsoknir/gagnasofn/
[380] The discussion does not extend to self-employed dentists, physiotherapists or psychologists.
[381] The Icelandic Act on Health Services no. 40/2007 (The Icelandic Health Services Act).
[382] The Icelandic Act on Health Records no. 27/2998 (The Icelandic Health Records Act) section 4 (2).
[383] Ibid. section 18.

seven health regions of Iceland are part of the interconnected structure.[384]

Within the different health care facilities, medical records are interconnected to support exchange of vital patient information. This enables health care providers to access health data at all stages of provision of care regardless of which facility delivers the services. The HealthNet Hekla (Hekla) is a closed and secure electronic communication network for health data exchange in Iceland.[385] Health care facilities can connect health record systems to Hekla for continuous exchange of health data and to interact and share information in a safe and reliable way.[386] Access to Hekla is subject to permit requirements and strict security procedures apply to ensure data security and confidentiality.[387] Iceland's infrastructure can be regarded interoperable, in this context meaning the ability of two or more electronic medical record systems exchanging computer interpretable data, and human interpretable information and knowledge.[388]

Despite the national standardization of health data through the interconnected system, health data is stored decentralized. Therefore, as for each relevant data controller, each health care provider must be approached to provide access to health data. This applies regardless of the purpose of processing.

10.2.2 Information resources

The role and responsibilities of health data information resources and other relevant authorities are regulated by law. This also include their mandate to grant access to health data or any involvement in the process. The main health data resources are the Directorate of Health (DoH), which includes the Chief Epidemiologist (CE) operating within the DoH, the National Archives of Iceland (NAoI), and Statistics Iceland. In addition, there are seven national biobanks[389], on being at the deCODE genetics, which is a global leader in analyzing and understanding the human genome that has gathered health data from over 160,000 Icelandic volunteers and leads the discovery of genetic risk factors for common diseases.[390] The non-governmental organizations, the Icelandic Cancer Society and the Icelandic Heart Association Research Institute, keep records for research and development. Other relevant authorities are the Data Protection Authority (DPA), the Medicines Agency (MA), the National Bioethics Committee (NBC)[391], and the Health Research Ethical Committees (HREC)[392] within two health care institutions.[393] In the following, as the same rules apply for the NBC and HREC's, reference will only be made to the NBC.[394]

No centralized system exists for administration of information requests and data permits for secondary use of health data.

Access is dependent on the approval of each data controller.

Even though health care professionals have direct access to individuals' health data for health care purposes and individuals have the right to access own health data, access for other purposes, such as scientific research, can be a complex and time-consuming process. Access for innovation and development are not specifically permitted by law.

There is no centralized system for administration of information requests and data permits for secondary use of health data. As access is subject to the approval of each data controller, innovators must often address multiple data controllers to access health data, typically with separate guidelines for access approval and application procedures. For example, access to health data for scientific research purposes is dependent on a permit from the NBC, provided the NBC has authorized the scientific research activities in question.

10.3 Legal reforms enabling secondary use

The Icelandic Government has focused on certain digitalization strategies to reach the goal of a more effective and innovative public sector. The National Centre for eHealth unit (eHealth unit) within the DoH is responsible for all national eHealth projects. The eHealth unit is responsible for standardization on a national level, as well as a national eHealth policy and implementation across Iceland. The national eHealth strategy for 2016-2020 includes four main objects.[395]

In recent years, an increased focus has been on providing individuals with guidance and enabling them to actively participate in their own treatment, including encouragement to take informed decisions on own health.

[384] Information from the DoH in February 2020.
[385] Owned by the DoH.
[386] The DoH: https://www.landlaeknir.is/um-embaettid/greinar/grein/item20338/Spurningar-og-svor-um-rafraena-sjukraskra
[387] The DoH's instructions on security and quality of health records from 2015: https://www.landlaeknir.is/servlet/file/store93/item27455/Fyrirmaeli%20landlaeknis%20um%20oryggi%20sj%C3%BAkraskraa%20(2).pdf
[388] Definition in point G 3 of the Commission's Recommendation on cross-border interoperability of electronic health record systems no. 2008/594/EC.
[389] The DoH register of biobanks: https://www.landlaeknir.is/um-embaettid/greinar/grein/item32062/lifsynasofn
[390] Decode Genetics, https://www.decode.is/thekking-i-allra-thagu/
[391] The Icelandic Act on Scientific Research within the Health Sector no. 44/2014 (The Icelandic Scientific Health Research Act) section 9 and 10.
[392] Ibid. section 11.
[393] Landspítali University Hospital and Akureyri Hospital.
[394] The Icelandic Scientific Health Research Act Section 10 (5).
[395] eHealth strategy: https://www.landlaeknir.is/servlet/file/store93/item28559/Rafr%C3%A6n_sj%C3%BAkraskra-og-heilbrigdisnet_Stefna-EL-til_2020_utg.2016_loka.pdf

To facilitate for this, Icelandic citizens are provided secure access to own medical records through the portal Heilsuvera.[396] Individuals can access limited parts of their medical records with electronic authentication, and view information about their prescriptions, vaccinations, allergies, laboratory results etc. Further, individuals can communicate with certain health service providers through Heilsuvera on a more frequent basis. Individuals can also insert own information, e.g. various measurements.[397] However, such data is not considered part of own medical records from a legal perspective.

Although there are no reports on the development of a new eHealth strategy, a health policy extending to 2030 (Health Policy) was recently adopted.[398] The Health Policy acknowledges innovation opportunities to promote health, as technological innovations in the health sector offer countless opportunities to improve quality and efficiency of health care.[399] It is underlined that the administrative and legislative framework within the health sector must provide sufficient flexibility for innovation and development.[400] The action plan for 2019-2023[401] includes the following objectives; open and accessible databases and biobanks for scientific researchers with required permits, establishment of a health science fund to provide funding for scientific research in the health sector, and establishment of a formal co-operation with the other countries and self governing territories in the Nordic region to evaluate new technologies and approaches.[402]

The Innovation Policy extending to 2030 (Innovation Policy)[403] aims at increasing legislation that supports competitiveness, as well as innovation.[404] Adaption of legislation to technological changes and ensuring Iceland can be first in line to implement technological innovations are recognized as important components in this regard.[405] The Innovation Policy also aims at ensuring publicly owned data is available to be used by anyone, provided privacy and data protection considerations are taken into account.[406] The Icelandic Science and Technology Council has acknowledged the importance of data for innovation, and that data is equally important for innovation as for research.[407]

The Report on the Future[408] discusses utilization of data and information in the health sector.[409] The report states that lack of consistent data utilization can create various threats[410], as well as recognizes the enormous opportunities within the health sector related to AI and other automation technology, which can spare resources, improve quality of service, and improve the quality of health care.[411] Furthermore, it is stated that to increase value creation in society during the fourth industrial revolution, in addition to strengthening education and basic technology skills, it is necessary to continue to build and promote innovation in a wide range of areas.[412]

The Icelandic government comprehend the importance of strengthening the entrepreneurial environment and has recognized promotion of innovation is necessary. However, no public discussions of enabling secondary use of health data for innovation and development purposes have occurred, nor have there been any proposals on adding this to the agenda.

> *When processing of health data includes an element of scientific research, the innovator must comply with the requirements under the Scientific Health Research Act*

10.4 General principles on use of health data

Health data is considered sensitive[413] and is subject to specific processing conditions.[414] The principal rule is that health data shall be processed only for the primary purposes the data originally was collected, meaning for provision of health care to individuals. For secondary use of health data for innovation and development activities, an innovator must have a legal basis for the processing[415], and must comply with the requirements in the Data Protection Act.[416] Examples of a legal basis is the data subject's consent[417] or a statutory provision in Icelandic

[396] Heilsuvera, https://www.heilsuvera.is/
[397] The DoH, https://www.landlaeknir.is/gaedi-og-eftirlit/heilbrigdisthjonusta/rafraen-sjukraskra/heilsuvera-minar-heilbrigdisupplysingar/
[398] The Health Policy: https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=879dd726-9e80-11e9-9443-005056bc4d74
[399] Ibid. p.12.
[400] Ibid. p.13.
[401] Health Policy Action plan 2019-2023 https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=0f999e52-99c2-11e9-9443-005056bc4d74
[402] Ibid. p.10.
[403] The Innovation Policy: https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=ae8c7637-eb68-11e9-944d-005056bc4d74
[404] Ibid. p.18.
[405] L.c.
[406] L.c.
[407] Minutes from the 38th Science and Technology Policy Council Meeting, October 3, 2019, p. 2 https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=39674700-1783-11ea-944f-005056bc530c
[408] The Prime Minister's Committee for the Future regarding challenges and opportunities stemming from technological changes 2035–2040, October 2019 https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=9c2eb35c-36c4-11ea-9456-005056bc4d74
[409] Ibid. p.16.
[410] Ibid. p.16 point G.
[411] Ibid. p.16 point H.
[412] Ibid. p.8.
[413] The Icelandic Act on Data Protection and the Processing of Personal Data no. 90/2018 (The Icelandic Data Protection Act) Section 3 (1) 3).
[414] Ibid. section 11.
[415] Ibid. section 9.
[416] Such as principles for the processing of personal data, cf. The Icelandic Data Protection Act section 8.
[417] The Icelandic Data Protection Act section 9 (1) 1).

law enabling processing of health data for innovation and development purposes.

When processing of health data includes an element of scientific research, the innovator must comply with the requirements of the Scientific Health Research Act. Processing of health data as a part of a clinical trial must be performed in line with the Pharmaceutical Act[418] and the Medical Devices Act[419], as well as any regulations adopted thereunder.

Access to data obtained within public health care is subject to the Information Act.[420] However, when data contains sensitive personal information or if access poses a particular risk of infringing the rights and freedoms of the data subject, access is limited. In these cases, the government must obtain an approval from the DPA before granting access. Such approval can be subject to detailed rules on access and safety standards.[421] Access is limited to research purposes.

10.5 Legislation

10.5.1 Introduction

In this context, the GDPR sets the basis for the understanding of the term 'health data'. There are different definitions of similar terms in Icelandic legislative acts, hereunder health information (heilsufarsupplýsingar[422] / heilbrigðisupplýsingar[423]), genetic information (erfðafræðilegar upplýsingar[424]) and health data (heilbrigðisgögn[425]). The understanding of the term 'health data' has not been debated by the DPA. Although the definitions somewhat vary, the interpretation of the GDPR and national legislation does not conflict.

In the following, user generated health data is covered by the term 'health data'. There are no special regulations in Icelandic legislative framework concerning user generated data. Therefore, the Data Protection Act applies to processing of such personal data.

10.5.2 Data protection

Through the EEA agreement, the GDPR was adopted to the Data Protection Act[426], which applies to the processing of personal data and regulates general aspects of data protection. Although the GDPR does not apply to the personal data of deceased persons[427], Iceland has adopted legislative measures allowing processing of personal data of deceased persons within the framework of the GDPR. Thus, the Data Protection Act regulates processing of personal data of deceased for a five-year period from their death or further when concerning personal data considered fair and reasonable to keep confidential.[428]

Sector specific data protection aspects are governed by multiple acts. There are sector specific data protection legislation, such as the Health Records Act and the Patient's Rights Act[429], as well as specific data protection provisions incorporated in other legislation, such as in the Scientific Health Research Act. The Data Protection Act does not apply provided there are special provisions in other acts on processing of personal data adopted within the framework of the GDPR. In these circumstances, these acts and the GDPR prevail.[430]

For processing health data, the basic principles[431] of the Data Protection Act must be complied with and a legal basis for processing is required.[432] As the Data Protection Act only applies to personal data[433], as a rule, processing of anonymous is not subject to the act. Data considered anonymous may be collected, registered, transferred, and stored without limitations.

> *The Data Protection Act applies to processing of user generated health data.*

Although the Data Protection Act provides alternative legal bases for processing of health data, not all legal bases provide ground for secondary use of health data for innovation purposes. Specific conditions apply for processing sensitive personal data[434], in which the basic principle is that the data subject explicit consent is required to process the data.[435] To serve as a legal basis, the data subject's consent must fulfil certain requirements. Further, in line with the alternative legal basis provided in the GDPR, there are several legal bases enabling processing of health data without the data subjects' consent. However, to apply these alternative legal bases, strict conditions must be fulfilled.

Reasons of public interests may serve as a legal basis covering, but not limited to, public health, scientific and historical research, and statistical purposes, as well as for

[418] The Icelandic Act on Pharmaceuticals no. 93/1994 (The Icelandic Pharmaceutical Act).
[419] The Icelandic Act on Medical Devices no. 16/2001 (The Icelandic Medical Devices Act).
[420] The Icelandic Act on Information no. 140/2012 (The Icelandic Information Act).
[421] Ibid. section 33.
[422] The Data Protection Act 3 (1) 3).
[423] The Biobanks Act section 3 (1) 14).
[424] The Data Protection Act section 3 (1) d).
[425] The Biobanks Act section 3 (1) 15).
[426] The Icelandic Data Protection Act section 2.
[427] The GDPR Recital 27.
[428] The Icelandic Data Protection Act section 4 (3).
[429] The Icelandic Act on Patient's Rights no. 74/1997 (Patient's Rights Act).
[430] The Icelandic Data Protection Act sections 5 (1) and 5 (3).
[431] Ibid. section 8.
[432] Ibid. sections 9 and 11.
[433] Ibid. section 4 (1).
[434] Ibid. section 11.
[435] Ibid. section 11 (1) 1).

preventive medicine, medical diagnosis, and the provision of health and social care or treatment. The processing must be considered necessary and carried out in accordance with law. Therefore, a supplementary legal basis, as required by the GDPR, should be sought after in Icelandic sector specific legislation. Such legal basis must provide suitable and specific measures to safeguard the fundamental rights and interests of the data subject. In terms of scientific or historical research, statistical purposes, and archiving purposes carried out in public interest, the Data Protection Act requires safeguard procedures and provides exemptions on such processing.[436] Appropriate safeguards, such as technical and organizational measures, shall protect the rights and freedoms of the data subjects and, in particular, ensure that the principle of data minimization is adhered to.[437]

For processing of health data for innovation purposes, an innovator must rely on the data subjects' consent. There are no supplementary legal basis addressing innovation specifically in the Data Protection Act. Thus, to assess whether the innovative activities can be based on another supplementary legal basis, innovators must refer to sector specific Icelandic law.

10.5.3 Professional secrecy

Duty of confidentiality applies to all employees in the health sector, health care professional, and other employees.[438] Health data acquired by health care personnel is subject to professional secrecy under the Health care Personnel Act, including trainees and non-health care personnel.[439] Non-health care personnel working within the health sector are subject to professional secrecy under the Public Administration Act.[440] Employees of biobanks are bound by duty of confidentiality.[441] To disregard professional secrecy, a legal basis for access to health data that exempts professional secrecy is required.

10.5.4 General regulation for health research

The Icelandic Act on Scientific Research within the Health Sector

In Iceland, the significant potential of using health data for scientific research is recognized by researchers and legislators. The Scientific Health Research Act regulates secondary use of health data and biological samples for scientific research within the health sector and applies to data research and research performed on human subjects.[442]

The legal framework sets strict requirements for the use of health data for scientific research, in which the act aims at promoting quality scientific research and safeguard the interests of participants.[443] The organization and conduction of scientific research must be ethical, scientific principles must be respected, and data protection safeguarded.[444]

Scientific research within the health sector is defined as a research on human subjects, biological samples, and where scientific methods are applied to health data to enhance knowledge of health and diseases.[445] Preparatory work does not stipulate any further information on the term scientific research or define how 'scientific method' should be interpreted. The terms 'innovation' and 'innovation and development' are not defined in Icelandic legislation or in the first Innovation Policy. 'Innovation company' is defined is a legal entity engaged in research or development activities.[446] Innovation and development activities can fall within the scope of the Scientific Health Research Act provided the activities include an element of scientific research.

A scientific research project must be approved by the NBC.

The DPA assesses the project's processing of personal data.

A scientific research project must be approved by the NBC.[447] Collection of, use of, and access to health data shall be in accordance with the research objective and the permit from the NBC.[448] The application period poses as a challenge for accessors, as the average processing time at the NBC is 26 days.[449] The DPA is involved as the relevant authority, and shall receive a summary of NBC's applications including the applicant's description of the processing of personal data that will be carried out for the purpose of the research.[450] The DPA assesses whether there are grounds for further examination of the application and provides NBC with a review. In necessary, instructions for processing are also provided. If the DPA considers the processing of personal data to violate the Data Protection Act, the NBC shall not issue a permit for the scientific research in question. The processing time

[436] Ibid. section 18.
[437] Ibid. section 18 (1).
[438] The Icelandic Patient's Rights Act section 12.
[439] The Icelandic Health Personnel Act section 17 (1).
[440] The Icelandic Act on Public Administration no. 37/1993 section 42.
[441] The Icelandic Biobanks Act section 11.
[442] The Icelandic Scientific Health Research Act section 2 (1).
[443] Ibid. section 1.
[444] Ibid. section 4 (2).
[445] Ibid. section 3 (1) 1).
[446] The Icelandic Act on Support to Innovation Companies no. 152/2009 section 3 (1) 3).
[447] The Icelandic Scientific Health Research Act section 12 (1).
[448] Ibid. section 16.
[449] Information from the NBC, March 2020.
[450] The Icelandic Scientific Health Research Act section 13 (1), cf. the Regulation on Scientific Research in the Health Sector section 7.

with the DPA is ten working days at the most. Once the DPA has processed an application, the NBC has ten business days to decide on whether to grant a permit.[451] Throughout the process, if the NBC or the DPA have any questions and/or comments for the applicant, the processing time can be delayed.

Further, the NBC authorizes access to health data for scientific research.[452] When authorizing access to biological samples, the donor's right to withdrawal should be taken into consideration, as well as individuals rights to restrict access to medical records.[453]

In addition to permit from the NBC and DPA, approval from each data controller is required.[454] To obtain approval from a data controller can also be a time-consuming process. The process can be prolonged if approval from multiple data controllers is required.[455]

> *Access must always be approved by the data controller.*

Regulation of clinical trials

Clinical trials of pharmaceuticals[456] are subject to the sections of the Pharmaceutical Act and regulations adopted thereunder[457], including preservation of health data obtained for human clinical trials. Permits from the MA and the NBC are required to perform clinical trial pharmaceuticals.[458]

In addition, clinical trials of medical equipment and the preservation of health data in this context are subject to the sections of the Medical Devices Act and regulations adopted thereunder. A manufacturer shall apply for clinical testing of medical devices to the MA, who is responsible for monitoring.[459]

10.6 Access to health data for secondary use

10.6.1 Access to health data in medical records

General

In Iceland, the legislation on medical records is comprehensive. Processing of health data in medical records is regulated by the Health Records Act, containing provisions in which health data can be processed without the individuals' consent. The provisions are based on a specific condition in the Data Protection Act[460], which means that Data Protection Act provides supplementary legal basis for processing. Regardless of where a legal basis for processing is founds, individuals are guaranteed certain rights under the Health Records Act. Individuals may object to storing identifiable health data in a health databank for scientific research purposes.[461] Further, individuals can restrict access to own medical record and sharing of information in interconnected medical records.[462]

All health care providers, public or private, are obliged to keep medical records.[463] As a principal rule, medical records shall be kept in an electronic form to the extent possible.[464]

Health care personnel involved in the treatment of a patient shall have access to the patient's medical records, although the access can be restricted.[465] An interconnected system allows health care personnel to access all medical records that have been entered into the system.[466] Icelandic citizens have a unique identification number and, with the option of interconnected systems, it is relatively easy to connect individuals' data from multiple sources. Thus, each citizen can have a coherent electronic medical record. Individuals consent for sharing health data among health care providers with interconnection for the purpose of providing health services is not required. However, the individuals have a right to opt out of an interconnection.[467]

Although national standardization of health care information structure through interconnection, the system is considered decentralized. Because health data is in multiple information resources, accessors must approach each health care provider to request access to medical records.

Access to medical records, regardless of the purpose, is prohibited unless an exemption is provided by law.[468] Medical records should be sent to public archives.[469] Please refer to this report section 10.6.4 for details on access to health data in Public Archives.

The data subject's consent and access to own medical records as a basis for secondary use

Individuals are provided with several rights in relation to their medical records. The individual, or a representative,

[451] Ibid. section 13 (2).
[452] Ibid. section 27 (1).
[453] Ibid. section 27 (3).
[454] Ibid. section 27 (2).
[455] There is no public information on the average time for the disclosure of collated data and the NBC does not have information on that.
[456] The Icelandic Pharmaceutical Act, section 1 (1).
[457] The Icelandic regulation on clinical trials in humans no. 443/2004.
[458] The Icelandic Pharmaceutical Act section 3 (1) 4).
[459] The Icelandic Medical Devices Act, section 9 (1).
[460] Ibid section 8 (1) cf. the Data Protection Act section 11.
[461] The Health Records Act section 17 A. That shall be recorded in their medical record.
[462] Ibid. section 19.
[463] Ibid. section 4.
[464] Ibid. section 4 (2).
[465] Ibid. section 13 (1).
[466] All public health care providers and most of the private are a part of this interconnected structure.
[467] The Health Records Act section 19.
[468] Ibid. section 12.
[469] Ibid. section 11.

have a right to access to medical records in whole or partly, as well to be provided a copy upon request.[470]

When access is not considered in the individual's interest, access is denied.[471] When health data is acquired from another source than the patient or health care practitioners, access approval from the data source is required.[472] The DoH may decide that the individual or its representative shall be granted access to the data, in whole or partly.

Icelandic citizens are provided secure access to their health data through the portal Heilsuvera, although medical records may include more information than accessible therein. It is not possible to download health data from the portal, for example to share it with an innovator. However, the data subject can share its content with whom they want, except for insurance companies.[473]

The Health Records Act does not regulate the preservation time of medical records. Instead, it refers to the Act on Public Archives.[474] Access to a deceased person's medical record is limited to close relatives, in which access is dependent on the presence of material reasons.[475]

When innovators are granted access to health data of deceased by close relatives, the Data Protection Act applies for processing of the data for five years after the individual's death.[476]

Access to medical records for the purpose of research

Access to medical records for scientific research is regulated by the Scientific Health Research Act.[477] The NBC authorizes access[478] to scientific researchers with permit to perform scientific research by the NBC.[479] In addition, access is dependent on the approval of the data controller.[480] For access to a joint medical record system or interconnected medical records, approval from each institution must be obtained separately.[481] The collection, use, and delivery of health data for scientific research shall be in accordance with the purpose of research and the permit provided by the NBC.[482] Each time a medical record is viewed for scientific research purposes, it must be recorded in the medical record in question.[483]

A patient or its representative can prohibit storage of health data in a health databank for scientific research purposes. Such prohibition shall be recorded in the individual's medical record.[484]

Provided the NBC has granted access to health data for scientific research, the NAoI can grant access to medical records and other records concerning health data of named persons.

Data from DoH's Prescription Medicines Register may be used in scientific research[485], in which access is subject to the provisions of the Patients' Rights Act, the Scientific research in the health sector, and the Data Protection Act.[486] The DoH shall issue procedural rules regarding access to the Pharmaceutical database.[487]

Access to medical records for quality assurance and health data analyzes

The DoH supervises quality monitoring and is authorized by law to have access to medical records for quality assurance and health data analyses.[488] A supervisor of medical records within a health care facility may grant health care personnel, other staff, and students undergoing vocational training in health care sciences,[489] access to medical records for purposes of quality development, and quality monitoring. The access is limited to the facility in question.[490]

10.6.2 Access to health data in national health registries

General

The DoH shall organize and maintain national registries on health, diseases, drug prescriptions, births, and the performance of health services. Maintenance is performed to gather information on health and health services, monitor services, ensure its quality, and assess its performance.[491] The data is provided by health service providers.[492] The national health registries can also be used for scientific research.[493] As a principal rule, personal identifiable data shall not be stored in the health

[470] The Health Records Act section 14 (1).
[471] Ibid. section 14 (3).
[472] Ibid. section 14 (2).
[473] The Icelandic Act on Insurance Contracts no. 30/2004 section 82 (2).
[474] The Health Records Act section 11.
[475] Ibid. section 15.
[476] The Data Protection Act section 4 (3).
[477] The Health Records Act section 17A.
[478] NBC's Procedures for Handling Applications for Access to Health Data no. 578 from 2018.
[479] The Icelandic Scientific Health Research Act section 27 (1).
[480] Ibid. section 27 (2)
[481] The DoH's instructions on security and quality of health records from 2015, p. 11.
[482] The Icelandic Scientific Health Research Act section 16.
[483] Ibid. section 25 (3).
[484] The Icelandic Health records Act section 17A.
[485] The Icelandic Pharmaceutical Act, section 27 (1).
[486] Ibid. section 27 (9).
[487] Ibid section 27 (10).
[488] The Icelandic Act on Director of Health and Public Health no. 41/2007 (Public Health Act) provides the DoH Access to medical records, cf. the Icelandic Health Records Act section 16 (2).
[489] Who have undertaken an obligation of confidentiality comparable to that of health care practitioners.
[490] The Icelandic Health Records Act section 17.
[491] The Icelandic Public Health Act section 8 (1).
[492] Ibid. section 8 (4).
[493] Ibid. section 8 (1).

registries.[494] Instead, all data shall be encrypted[495] and in general, all processing of data should be in an encrypted form. In some circumstances, the data may be decrypted, for example when it is necessary for statistical or scientific research purposes, in which privacy is assured by appropriate measures.[496]

The data can be personally identifiable upon the data subject's consent.[497] However, the DoH may include data subjects' names, identity numbers, and similar identifiable information without the patient's consent in eleven health registers listed in the Public Health Act.[498] At the time of this report, there are nineteen national health registries[499] at the DoH, in which DoH is the data controller.[500] In some circumstances, other legal entities are considered data processors.[501]

Health registry data may only be accessed for scientific research purposes.

Secondary use of health data from national health registries

Access to identifiable information from the eleven national health registries for scientific research purposes is regulated by the Scientific Health Research Act.[502] The NBC authorizes access to health data for scientific research purposes, provided prior approval by NBC is obtained for the research activities in question.[503] A DoH research data committee evaluates the specific access applications.[504] All use of information from health registries shall be in accordance with the health registers' purposes.[505] Access to health data from health registries for other purposes than scientific research is not possible under Icelandic legislation.[506] Without a permit from the NBC, the DoH can only provide anonymized data in the form of statistics.[507]

10.6.3 Access to health data in biobanks

General

The objective of the Biobanks Act[508] is to establish a framework for the collection, keeping, handling, and utilization of biological samples from human beings, as well as ensuring confidentiality, the interests of donors of biological samples, the purpose of science and medicine, and public good. Iceland has established databases and biobanks containing data on diseases and health of its citizens.[509] The DoH has a register of biobanks[510], which contain inter alia information on the membership of the governing board of each bank, and the identity of the responsible party. At the time of this report, there are eight biobanks with license from the MoH.[511] There is no central entry point and register providing data on a sample level for the Icelandic biobanks.

Under Icelandic law, it is distinguished between a service research[512], scientific health research[513], and biological samples, in which the categorization is dependent on the purposes for which they are collected. Biological samples are defined as organic material from a human being, alive or deceased, which may provide biological information about the individual.[514] Biological samples are acquired for a scientific purpose[515] and for the purpose of health services to the individual.[516] Biological samples shall be stored without personal identification in accordance with the rules of the DPA.[517] Unlike in Norway, a distinction between treatment biobanks and research biobanks is not made.

The licensee of a biobank[518] is not considered the owner of the health data.[519] The licensee is entitled to dispose of the health data, with the limitations laid down by law, but is unauthorized to sell or transfer health data materials to another party.

Access to health data in biobanks is dependent on a permit from NBC.

[494] Ibid. section 8 (1).
[495] Ibid. section 8 (3).
[496] The Icelandic Regulation on Health Registries no. 548/2008 (The Icelandic Regulation on Health Registries). section 26 (2)
[497] The Icelandic Public Health Act section 8 (1).
[498] Ibid. section 8 (2).
[499] DoH, https://www.landlaeknir.is/tolfraedi-og-rannsoknir/gagnasofn/
[500] The Icelandic Public Health Act section 8 (4).
[501] For example, the Icelandic Cancer Society is the processor of the Cancer Register and the Gynecology department at the National University Hospital is the processor of the Birth Register.
[502] Ibid. section 8 (8).
[503] The Icelandic Scientific Health Research Act section 27 (1).
[504] The DoH: https://www.landlaeknir.is/tolfraedi-og-rannsoknir/rannsoknir/adganguradgognum/
[505] The Icelandic Regulation on Health Registries section 28.
[506] According to the Icelandic Health Register Act and the Regulation.
[507] Information from the DoH May 2020.
[508] Icelandic Act on Biobanks and health data collections no. 110/2000 (The Icelandic Biobanks Act).
[509] deCode: https://www.decode.com/research/
[510] The Icelandic Regulation on the preservation and utilization of Samples in Biobanks no. 1146/2010 (The Icelandic Regulation on Samples in Biobanks) section 14.
[511] DoH, https://www.landlaeknir.is/um-embaettid/greinar/grein/item32062/lifsynasofn
[512] The Icelandic Regulation on Samples in Biobanks section 2 (1) 5).
[513] Ibid. section 2 (1) 4).
[514] The Icelandic Biobanks Act section 3 1).
[515] Ibid. section 3 3).
[516] Ibid. section 3 4).
[517] Ibid. section 8 (1). The DPA rules from 2019: https://www.personuvernd.is/log-og-reglur/reglur-og-reglugerdir/reglur-um-oryggi-vid-medferd-og-vardveislu-lifsyna-i-lifsynasofnum
[518] A licensee is an individual or legal entity that has been granted a license by the MoH to operate a biobank cf. the Biobanks Act section 4.
[519] The Icelandic Biobanks Act section 10 (1).

Secondary use

As a principal rule, gathering health data and biological samples shall be obtained for clearly stated and legitimate purposes only.[520] No distinction is made between research samples and clinical samples in this regard. However, certain exceptions relevant to scientific research[521] apply upon the fulfilment of certain conditions. For example, a licensee of a biobank can provide access to biological samples to others for further diagnosis of diseases and development of methods.[522] This indicates that an innovator can be provided access to the health data, provided the innovative activities can be considered further diagnosis of diseases. However, preparatory work implies that the exceptions are only applicable for research purposes with the approval of the NBC.[523] Further, the licensee may grant access to biological samples for purposes of quality control, development of methods, and teaching, provided that the samples does not identifiable information.[524] Access is dependent on a permit from the NBC, provided the NBC has authorized the scientific research.[525]

When access to biological samples originally acquired for the purpose of health services is permitted for scientific research purposes, in general, the samples shall be provided without identifiable information. Samples including identifiable information shall only be permitted on an exceptional basis, in which the permission of the DPA is required.[526]

The Board of the relevant Biobank may authorize the use of biological samples for other purposes,[527] provided that urgent interests are expressed, and the benefits of use outweigh the potential inconvenience to the donor or other parties. In addition, permission from the DPA is required.

10.6.4 Access to health data in national archives

General

There is an obligation to preserve and transfer medical records to public archives at the NAoI.[528] The role of public archives includes making archives available for scientific research and facilitate research to the possible extent.[529] No mention of facilitating innovation and development is made.

Public bodies are obligated to transfer all records to the NAoI.[530] The same applies to private legal entities undertaken operational projects under contract.[531] When records reach 30 years of age, they shall be sent to the NAoI. However, electronic documents shall normally be delivered no later than after five years.[532] Generally, once transferred, the responsibility for the custody of the documents is transferred to a public archive.[533] However, entities subject to a transfer obligation shall retain responsibility for handling and granting access to information from electronic records until the records reach 30 years of age. [534]

At the time of this report, data is stored at health care facilities until the individual is deceased.[535] Exception is made for when doctors resign from private practices[536], in which medical records are transferred to the NAoI. In these circumstances, health data are archived in the NAoI, resulting in health data of living individuals not being part of the interconnected system.[537] The method of transfer vary between the different health care facilities. For example, at the time of this report, the NAoI has not received any electronic medical records.[538] When requesting access to information regarding a specific person including name and identification number, the NAoI cannot easily find the data.

> *The National Archives' role does not encompass facilitation of innovation and development.*

Secondary use

Upon request, the NAoI is required to provide the public with access to documents 80 years from the time they were created. Access to health data is included but is subject to certain requirements. Access to medical records and other records concerning health data of named persons can only be granted 100 years after the date of the last entry in the record.[539] Disclosure of data for scientific research purposes represents an exception in this regard. Disclosure must be necessary for scientific research, and protect the data subject's rights or other equivalent reasons.[540] An application must be submitted to the Data Protection Authority, which will evaluate the

[520] Ibid. section 9 (1).
[521] Stipulated in The Icelandic Biobanks Act section 9 (3) – section 9 (7).
[522] The Icelandic Biobanks Act section 9 (2).
[523] General comments on section 9 of the Icelandic Biobanks Act.
[524] The Icelandic Biobanks Act section 9 (2).
[525] Ibid. section 9 (4).
[526] Ibid. section 9 (5).
[527] Other than specified in the Icelandic Biobanks Act section 9 (2) – 9 (4).
[528] The discussion only applies to the NAoI not regional archives cf. section 9 of the Icelandic Act on Public Archives no. 77/2014 (Public Archives Act).
[529] The Public Archives Act section 13.
[530] Ibid. section 14.
[531] Under the Icelandic Act on Public Finance, cf. the Icelandic Public Archives Act section 14 (1) 7.
[532] The Icelandic Public Archives Acts section 15 (1).
[533] Ibid. section 22 (5).
[534] Ibid. section 15 (1).
[535] Information from the NAoI in April 2020.
[536] The NAoI: https://skjalasafn.is/sjukraskrar
[537] Provided the doctor was a part participating in the sharing network, which is voluntary, cf. this report section 10.2.1
[538] Information from the NAoI in April 2020.
[539] The Icelandic Public Archives Act section 26 (3).
[540] Ibid. section 31 (1).
[540] Ibid. section 32 (2).

application with respect to the nature of the information, as well as the purpose of disclosure.[541] The Public Archives Act does not contain specific rules on access to anonymized data.

Anyone gaining access to restricted health data from the NAoI is bound by confidentiality and may not display, forward, or otherwise use the information in any other way than laid down in the license from the public archives.[542]

Access to health data for innovative activities from the NAoI is limited because of time restrictions in law. In addition, there are no exemptions for anonymized data.

economy and society.[543] A great amount of data collected by Statistics Iceland is publicly available.

Statistics Iceland shall distribute its data for statistical scientific research.[544] For that purposes it can grant a certified or a trustworthy researcher[545] access to data with general information about individuals, provided personal identifiable information has been removed.[546]

Stricter conditions apply to access sensitive personal information[547], in which specific conditions for processing according to the Data Protection Act must be fulfilled.[548] Additionally, upon completion of a research project, the researcher must return the data, or delete any personal

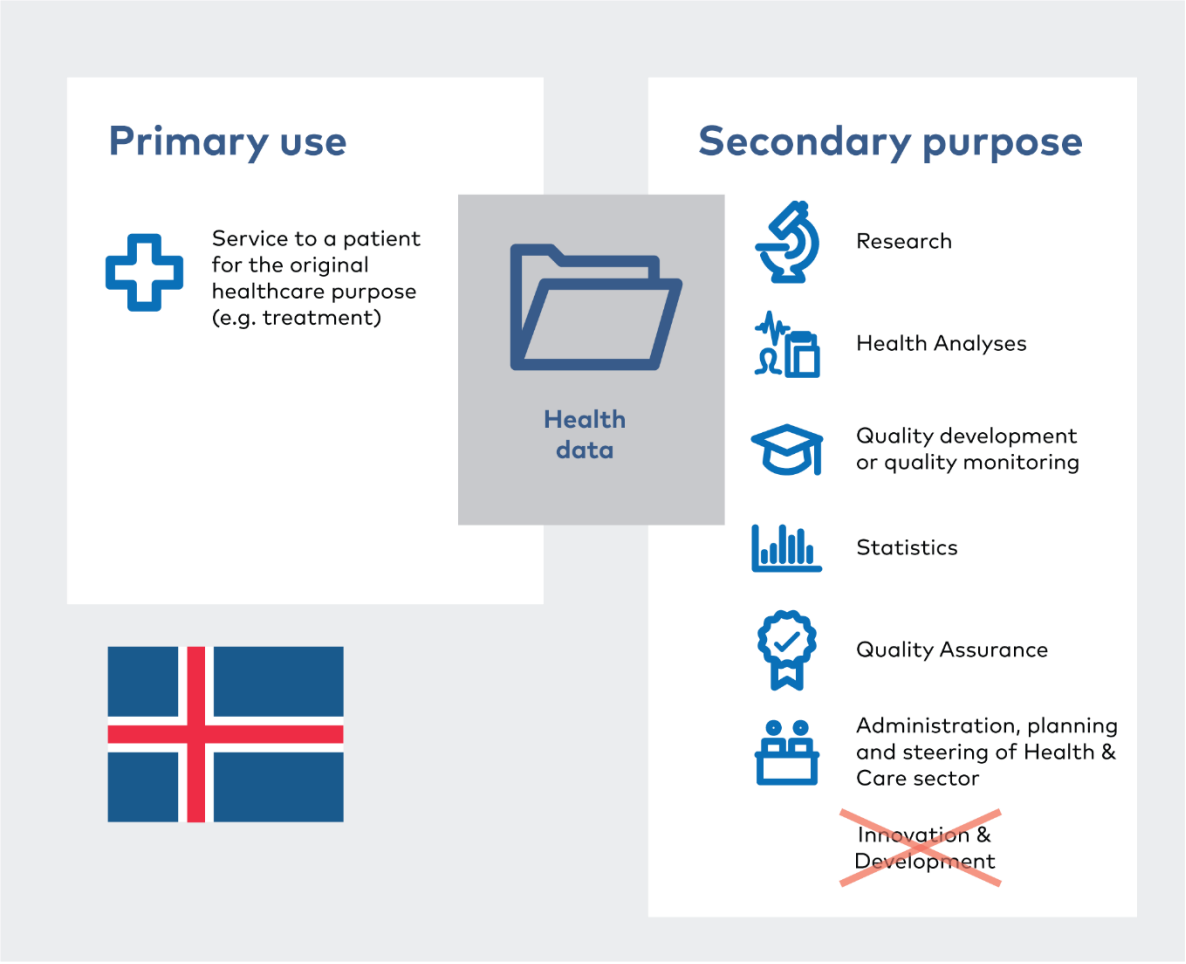


Figure 8 - Regulated division of primary and secondary use of health data in Iceland

10.6.5 Statistics Iceland

Statistics Iceland is the National Statistical Institute, which collects, processes, and distributes data on the

identifiable information from the data [549] The Icelandic Act on Statistics Iceland does not reference granting data for

[541] Ibid. section 32 (1).
[542] Ibid. section 33.
[543] The Act on Statistics Iceland no. 163/2007 (The Statistics Iceland Act) section 1 (1).
[544] Ibid. section 13 (1).
[545] The terms are not defined in the Statistics Iceland Act.
[546] The Statistics Iceland Act section 13 (1).
[547] Ibid. section 13 (2).
[548] The Icelandic Data Protection Act section 11.
[549] The Statistics Iceland Act section 13 (2).

innovation purposes. Thus, innovators can only access publicly available health data.

10.7 Transfer of and transborder access to health data

10.7.1 Transfer of health data across the Nordics

Generally, personal data is subject to free movement, provided there is a legal basis for the transfer. There are certain special provisions in Icelandic legislation regarding transfer of health data across national borders. For example, a permit from the NBC is required if the transfer is for scientific research purposes.[550] The NBC may also authorize a transfer of health data when granting access to health data for scientific research in the health sector.[551] Further, transfer of biological samples and health data from Iceland for scientific research purposes in the health sector is subject to the Data Protection Act.[552] A biological sample may be transferred across national borders for certain purposes, hereunder that the transfer must be in the donor's interest, and be conducted for diagnosis or quality control.[553] The transfer of biological samples, service samples, and research samples for research purposes is subject to the approval of the NBC and the DPA.[554] Transfer of scientific samples is also subject to the approval of the responsible research licensee.[555]

There are no other sections in Icelandic health legislation mentioning transfer of health data across national borders or that specifically enable, set restrictions, or prevents cross border transfers. Consequently, transfer of health data from Iceland for any other purposes than the above mentioned can occur, provided in accordance with the Data Protection Act and the GDPR.[556]

Transfer of health data for scientific research purposes require a permit from the NBC.

Transfer for other purposes must comply with the GDPR.

10.7.2 Transborder access to health data

To facilitate for cross border patient mobility, entailing that Nordic citizens' health data is available upon provision of health care, transborder access to health data must be ensured and interoperability is necessary.[557] The interconnected electronic medical records that Iceland has implemented on a national level enables seamless exchange of vital patient information among Icelandic health care providers.[558] The Health Records Act does not specifically require that such an interconnected system is restricted to Icelandic health care providers only, meaning it does not prohibit a connection across national borders or require data subjects consent for a cross-border access.[559]

Icelandic legislation does not hinder transborder access to health data through interconnections, provided the health care providers security system meets the DoH quality and security requirements.[560] Thus, as long as it has established an effective security system that meets the quality and security requirements of the DoH, it is technically possible to interconnect any health care provider in the Nordics with the Icelandic electronic medical records.[561] Records viewed in an interconnected health information system are not copied or automatically saved to the viewer's database. However, the direct viewing can be considered a transfer under the GDPR.

Even though there could be transborder access to Icelandic health data through interconnection, the Health Records Act applies to treatment provided in Iceland only.[562] Thus, health care professionals in other countries and self governing territories in the Nordic region may not enter Icelandic medical records when treating an Icelandic patient. To enter the Icelandic patient's medical record in the Icelandic system, the health care professional in question must be licensed by the DoH as a legally recognized health professional.[563] Citizens from other countries or self governing territories in the Nordic region can apply for a license at the DoH, as their professional qualifications could be recognized in Iceland.[564] However, this rights does not affect the health care professional's ability to enter health data in Icelandic medical records,

[550] The Icelandic Scientific Health Research Act section 12.
[551] Ibid. section 27.
[552] Ibid. section 8.
[553] The Icelandic Biobanks Act section 10 (3).
[554] The Icelandic Regulation on Samples in Biobanks section 12 (1).
[555] Ibid. section 12 (2).
[556] The Icelandic Data Protection Act section 16.
[557] Interoperability is defined in this context as "the ability of different information systems to connect to access, exchange and use patient data to optimize the health of individuals.": https://www.nordicinnovation.org/programs/nordic-interoperability-project
[558] A distinction is made between an interconnected health information system and a joint health information system. When health information systems of two or more controllers are interoperable in such a way that data from medical records may be shared between the systems it is interconnected. In that case each data controller is responsible for the data processing of the medical records and being consistent with sections of the Icelandic Health Records Act and the Icelandic Data Protection Act. However, when two or more health care facilities have a joint health information system, there is only one data controller, the health care facilities have agreed on.
[559] The Icelandic Health Records Act section 18, describes the authorization to interconnect health information systems. The supervisor of medical records that has the authority to grant the access, but quality and security requirements made by the DoH must be met.
[560] The DoH's instructions on security and quality of health records from 2015: https://www.landlaeknir.is/servlet/file/store93/item27455/Fyrirmaeli%20landlaeknis%20um%20oryggi%20sj%C3%BAkraskraa%20(2).pdf
[561] Information from the team manager of the Icelandic electronic health record at the DoH.
[562] The Icelandic Health Records Act section 1 (2).
[563] Ibid. section 3 (1) 10.
[564] By Directive 2005/36/EC, in Act no. 26/2010 on the recognition of professional qualifications for the pursuit of an activity in Iceland.

when working with an Icelandic patient from a health care institution in the Nordics.

10.8 National obstacles

10.8.1 Lack of innovation specific regulation

Access and use of health data for innovation and development purposes is not regulated in a holistic manner in Iceland. Thus, there is no explicit legal basis for secondary use of health data for innovation and development activities in Icelandic legislation, other than data subject's consent, which constrains innovative activities. Therefore, the legal basis for processing non-anonymized health data for innovative purposes must be based on the data subject's explicit consent. Further, consent presents some practical considerations and obstacles which can be difficult to overcome. Please refer to section 13.2.1 for details on the challenges reliance on consent presents.

10.8.2 Decentralized system

Health data in Iceland is stored decentralized managed by several data controllers. Iceland does not have a centralized system in place for the collection of health data, anonymized or non-anonymized, nor a centralized authority that administrates data requests and enables access to data from multiple sources.

The Icelandic legislation provides a legal basis for access to health data for research purposes under certain conditions. The NBC must grant a permit for scientific research, as well as permission to access health data. As access is subject to the approval of each data controller and scientific researchers are required to contact multiple data controllers to collect data, the system can be described as cumbersome. The administrative burden is caused by multiple laws regulating access and use of health data for scientific research, and poses as an obstacle for scientific researchers, as well as for innovators.

10.8.3 Lack of interoperability of electronic medical records

Health care facilities are not required by law to have interconnected electronic medical records. Evidently, it is difficult to ensure a fully interoperable system for sharing of health data. Further, as it is not mandatory to keep medical records electronically, and the legislation only states this shall be done to the extent possible, records are kept in different formats.

Due to lack of fully electronic and interoperable national systems, it is difficult to promote such on a Nordic level. However, standardization is a requirement for a successful exchange of health data across borders, enabling data portability of user generated data form health databases and registries, secondary use of such compiled data sets, and support patient mobility between the Nordics. Further, a legal basis for the transfer must be ensured.

10.8.4 Data portability for user generated data

Although individuals have a right to data portability under the Data Protection Act, the existing legal framework does not enable individuals to enter user generated data into their medical records. Health personnel are the only ones that have authority to enter information to medical records and only in relation to treatment provided in Iceland. This may limit utilization of user generated data in a health care perspective and may hinder establishment of a fully centralized information system for accessing health data.

10.8.5 Restricted access to medical records of deceased

The Data Protection Act applies to processing of personal data of deceased up until five years after their death. However, only public entities transfer health data of deceased to the NAoI. Further, how active health care facilities preserve medical records and transfer them to NAoI differs. At the time of this report, the NAoI has yet to receive any electronic medical records. Thus, innovators' access to health data of deceased appears unclear and limited.

11. Norway

11.1 Introduction

There are several information resources for health and other personal data in Norway. These information resources are considered to be significant and important for the future of Norwegian health care.

Most health data in these information resources originate from provision of health care, which in this context is regarded as primary use of health data and is subject to strict rules on professional secrecy. Thus, use of health data for other purposes than health care is allowed only on an exemptional basis. Such use is regarded as secondary use. As health data is personal data, the processing of such data must comply with the GDPR thus, a valid legal basis for any purpose of secondary use must be in place.

Although processing of health data for innovation and development is crucial for the future of health technology, according to statistics on disclosure of health data from Norwegian health registries, disclosure of health data for commercial purposes in Norway appears to be limited.[565] The numbers show that Health industry research is conducted mostly in collaboration with academic institutions, such as universities. In this chapter we will analyze and assess the existing possibilities for access to and use of health data for commercial purposes as innovation and development.

There are no explicit regulations on access to health data for innovation and development activities which means that access and further processing is mostly depended on the data subjects' consent. The data subjects' consent may be a suitable legal basis in some innovation projects, especially when there is direct contact with the data subject through trials, testing of wearables, apps, etc., as regarding access to immense amounts of health data for AI-performed analysis, consent may be challenging especially when it comes to number of data subjects.[566] Thus we will also assess whether processing of innovation and development may be included by regulation aimed at use for other purposes.

Under Norwegian law, there are no provisions in general regulating or preventing processing of health data across national borders. In general, any innovators, researchers or other enterprises established outside Norway may access and process health data on the same terms as nationals.

11.2 Norwegian health care system and information resources

The Norwegian state has the principal responsibility for providing health care to the public, while the municipalities are responsible for actual provision of primary health and social care. Specialist care is provided under the auspices of the Ministry of Health care Services through ownership in hospitals. Alongside the public sector, consisting of several governmental agencies and organizations, private health service providers contribute to the maintenance and development of the health care sector.[567]

All health care providers, both public and private, are obliged to keep medical records. Today, medical records are kept electronically.

In addition to medical records, there are several significant sources for health and other personal data in Norway. Valuable health data is found in biobanks, health registries and national health surveys, public archives, quality registries in the health care sector, and in Statistics Norway's databases. The role and responsibilities of the most important information resources and relevant authorities for health data is regulated by law, hereunder the Directorate of Health, Directorate of eHealth, National Institute of Public Health (NIPH), the Cancer Registry, Statistics Norway, the Norwegian Labour and Welfare Directorate, Norwegian Medicines Agency, Regional Committees for Medical and Health Research Ethics (REC), National Research Ethics Committee for Medicine and Health Sciences (NEM) and the Norwegian Data Protection Authority (the Norwegian DPA).

There are established several metadata portals and registries to provide an overview of existing information resources, such as the biobankregisteret.no, helsedata.no At the time of this report, no national data catalogue exists.

11.3 Legal reforms enabling secondary use

In recent years, the Norwegian government has launched several initiatives to improve, simplify and modernize access to health data.

[565] Consept evalution - the Health Analysis Platform, The Directorate on Ehealth (April 2018).
[566] Cf. this report chapter 4.
[567] The term 'health care sector' will in this report refer to the municipal health care services, the specialist health services, dental services and private providers of health care services, cf. the Norwegian Patient and User Rights Act of 2 July 1999 (The Norwegian Patient and User Rights Act) section 1-3 d).

In 2017, the government adopted a National strategy for access to and sharing of research data.[568] In the same year, Helsedatautvalget (the Health Data Committee) published the report *A new system for easier and more secure access to health data*.[569] Among other things, the Health Data Committee concluded that improved access of health data for secondary use can be achieved through the establishment of a health analysis data program and a health analysis platform, as well as through realization of the Summary Care Record[570]and the long-term strategy named 'One Patient One Record'.

In March 2017, the Summary Care Record was established. The record contains important information about a person's health, such as allergies, medical history etc. and is available to all Norwegian citizens. The record can also be accessed by health personnel if a person requires medical care.[571] In December 2018, it was decided to establish a health analysis platform.[572] This will simplify access to health data for secondary use through a data platform containing copies of data from Norwegian health registries, health surveys and biobanks. The platform will also enable health analyzes without identifiable personal data being visible to the analyst.[573] In December 2019, the first version of Helsedataservice, a centralized access service, was launched. The service coordinates applications for access to data from health registries controlled by the Directorate of Health, the Cancer Registry and the NIPH.

In the spring of 2020, the government proposed certain amendments of the Health Register Act.[574] If adopted, the amendments will provide the health analysis platform and Helsedataservice with a legal basis for use of health data from national health registries. The health analysis platform will provide for improved facilities for conduction of analysis in a secure environment, embedding privacy by design and adequate information security. The proposed amendments will also provide a legal basis for secondary use of health data in statistics, health analyzes, research, quality improvement, planning, and management to promote health, prevent disease and injury, and provide better health and social care services. Further, the legal bases for access to the national health registers should be included directly in the provision of the Health Register Act. As for now the legal bases are laid down in specific regulations for each register. A proposal to vest the power to exempt from the professional secrecy in one authority only, is also included. Among others, the aim is to provide improved and more secure treatments and health and social care services to the public, as well as to increase access to health data to facilitate for innovation and business development.

Further, the Norwegian government has proposed an act on e-health. [575] By facilitating for digitalization in the health care sector, the act will contribute to effective and secure health and social care services. It provides a legal basis for a national health portal for the citizens of Norway (helsenorge.no). The portal aims at facilitating for access to own health data, self-service and electronic communication with the health sector. If adopted, it will be mandatory for relevant actors in the health sector, such as municipalities, county municipalities, health enterprises and businesses, to consider the need for national cooperation and interaction when working with different e-health solutions. This will increase the interoperability within Norwegian e-health solutions.

Helsedataservice as a centralized access service was launched in December 2018.

11.4 General principles on use of health data

Health data is a special category of personal data under the GDPR. Thus, as a main rule, health data shall only be used for the purposes the data originally was collected for. For innovators, a legal basis in the GDPR is always required to process health data, as well as compliance with the other requirements in the GDPR. Please refer to this report chapter 4.

As a starting point, all personal data obtained within public health and medical care can be accessed pursuant to the Freedom of Information Act.[576] However, when information is subject to statutory or secrecy, which health data is, the right to access is limited. Health care personnel are subject to professional secrecy under the Health Personnel Act. The duty involves that all health care personnel are prohibited from disclosing information regarding a patient's health to others, unless the patient consents to such disclosure or there are any statutory exemptions permitting such disclosure.

[568] Nasjonal strategi for tilgjengeliggjøring og deling av forskningsdata, Kunnskapsdepartement, F-4442 B, (12/2017)
[569] Et nytt system for enklere og sikrere tilgang til helsedata, Rapport fra Helsedatautvalget 2016-2017, I-1179 B (09/2017)
[570] 'Kjernejournal'.
[571] Regulation on the Summary Care Record (FOR-2013-05-31-563).
[572] The Directorate on Ehealth, https://ehelse.no/programmer/helsedataprogrammet/helseanalyseplattformen
[573] Prop. 63 L (2019–2020) Amendments to the Health Registry Act, etc. (access to health data) section 6 (1).
[574] Prop. 63 L (2019–2020). The bill is pending in Parliament. In this preparatory works the term health data includes both personal data concerning health and anonymous data on peoples' health, but there are not any proposals that will alter the definition of data concerning health as set in the GDPR.
[575] Prop. 65 L (2019–2020) The Act on ehealth.
[576] The Norwegian Act relating to the right of access to documents held by public authorities and public undertakings of 19 May 2006 (The Norwegian Freedom of Information Act).

A decision exempting professional secrecy is regarded a supplementary legal basis under the GDPR

If the processing of health data is regarded as health research, the innovator must comply with the requirements within the Health Research Act and the Research Ethics Act, cf. this report section 11.6. Processing of health data as a part of a clinical trial must be performed in line with the Regulation of Clinical Trials on Medicinal Products for Human Use.

Transfer of personal data is regulated by the articles of the GDPR, which requires free movement of data within the EEA, provided there is a legal basis for the transfer. Please cf. this report section 4.7.

11.5 Legislation

11.5.1 Data protection

The GDPR is incorporated into Norwegian legislation by the Norwegian Personal Data Act.[577] Thus, processing of health data must comply with the conditions in the GDPR.

The act supplements the articles of the GDPR and provides both additional conditions and legal bases for processing of ordinary and special categories of personal data necessary for scientific research or statistic purposes, without the consent of the data subject.[578] The processing purpose must be in the interest of the public, which must clearly exceed the processing's disadvantages for the individual. The controller is obliged to consult the data protection officer to assess whether the processing of personal data satisfies the requirements of the Data Protection regulation and other applicable regulation.[579] There is no similar legal bases in the Norwegian Personal Data Act as regards processing of personal data for innovation and development.

11.5.2 The professional secrecy

As mentioned above, health data processed by health personnel is subject to professional secrecy.[580]

Health data deriving from health personnel's activities covered by different laws are also subject to this duty i.e. processing of health data in medical records,[581] within the municipality health and social care services[582] and specialist health care services,[583] in health registries,[584] and in research projects[585].

Exemptions from the duty of professional secrecy is laid down in several acts. These exemptions enable access to health data for certain secondary use purposes, without consent from the data subject.

11.6 General regulation on health research

11.6.1 General

When conducting research involving health data, some general requirements in different legislation must be followed. This will also apply to innovators' research activities.

Further, several provisions in different acts provides legal basis for researchers access to health data collected in the health and social care sector or by the Public Administration, without the data subject's consent. Although Norwegian legislation recognize in general scientific research as a valid purpose for secondary use of health data and provide this purpose with the necessary legal basis, there is no mention of innovation. To assess whether access is allowed for innovation purposes, one must to assess whether any of the exceptions available for scientific research purposes apply. In this regard, the relationship between innovation and research is of importance.

Professional secrecy may pose as an obstacle for innovators' access to health data. However, health data can be accessed upon the data subject's consent.

11.6.2 The Health Research Act

The Health Research Act provides requirements regarding the research organization and conducting of the research in question, but the act also regulates access to and processing of health data.

The Health Research Act applies to medical and health research on humans, human biological material or health data. Medical and health research is defined as *"activities*

[577] The Act on the Processing of Personal Data of 15 June 2018 (The Norwegian Personal Data Act). The GDPR and The Norwegian Personal Data Act are collectively referred to as the Data Protection Regulation.
[578] Ibid. section 8 and 9.
[579] Ibid. section 10.
[580] The Norwegian Act relating to Health Personnel etc. of 2 February 1999 (The Norwegian Health Personnel Act) section 21 and 21a.
[581] The Norwegian Act on Health Records of 20 June 2014 (the Norwegian Health Records Act) section 15.
[582] The Norwegian Act Relating to Municipal Health and Care Services of 24 June 2011 (The Norwegian Health and Care Services Act) section 2-1.
[583] The Norwegian Act on Specialists Health Service of 2 July 1999 (The Norwegian Specialist Health Service Act) sections 1-1 and 1-2.
[584] The Norwegian Act on Personal Health Data Filing Systems and the Processing of Personal Health Data Norwegian of 20 June 2014 (the Norwegian Health Register Act) section 17.
[585] The Norwegian Act on Medical and Health Research of 20 June 2008 (The Norwegian Health Research Act) section 7.

Medical and health research is defined as activities using scientific methodology to provide new knowledge concerning health and diseases.

carried out using scientific methodology to provide new knowledge about health and disease".[586]

The term 'scientific methodology' is intended interpreted broadly but excludes activities that does not involve any systematical work or does not produce any findings suited for generalization.[587] If the activities in question are regarded systematic and apply existing knowledge from research and practical experience to develop new or improve existing products, processes, systems and services, it is natural to characterize the activities as research within the scope of the act.[588]

For use of health data for innovation and development within the scope of the act, strict requirements regarding the organization of the project and research activity in question will apply regardless from which information source the relevant health data originate. For example, it is required that the research project has a natural or legal person responsible for the project, in addition to a project manager. This project manager must inherent professional and scientific competence.[589] For projects lead by innovation companies, and not by traditional research institutions, it may pose as a challenge to fulfil all requirements. Upon application for access to register data, actors from the health industry are typically listed as a sponsor or client, as they are interested in the research results, while academic institutions are listed as research managers.[590] Which means that access for projects lead by innovation companies are rare, probably due to these requirements.

All research projects within the scope of the act require prior approval from REC[591] and all processing of health data must comply with the GDPR. In addition, the degree of personal identification in the health data being processed must not be greater than is necessary to serve the purposes.[592]

Participation of research subjects is generally based on consent, the reasons being both research ethics and privacy. The act opens of for the concept of a so called 'broad consent', which allows research participants to consent to use of their human biological material and health data for *"...broadly defined research purposes"*.[593]

This type of consent is considered to be in line with the GDPR. Consent is not required for processing of anonymized data or anonymous human biological material.

11.6.3 Research Ethics Act

The Research Ethics Act requires research to be conducted in accordance with recognized norms of research ethics.[594] If the innovation activity is regarded as a health research project, consequently the Research Ethics act will apply. The act also imposes a duty on research institutions to ensure that research at the institutions is conducted in accordance with these norms. How to process data, hereby personal data, within the framework of the GDPR and the duty of professional secrecy is regarded as such norms.

Research institutions are public or private institutions that have research as their main task.[595] The act's application is limited to researchers and research in Norway, and when the research is conducted by researchers employed by a Norwegian employer or if a significant part of the funds come from Norway.

11.6.4 Regulation of Clinical Trials on Medicinal Products for Human use

Clinical Trials on medicinal products for human use (clinical trials) are regulated by both national and international laws, hereunder by the European Directive 2001/20/EC, the GDPR, and the Regulation Relating to Clinical Trials on Medicinal Products for Human Use.[596]

As clinical trials involve processing of health data, the articles of the GDPR concerning processing and the Health and Research Act apply. Please refer to this report chapter 4 for details on the GDPR.

When applying the concept of broad consent, research participants can allow use of their personal health data for specific and broadly defined research purposes.

[586] Cf. The Norwegian Health Research Act section 4 b).
[587] Ot.prp.nr.74 (2006–2007).
[588] Ot.prp.nr.74 (2006–2007), section 9.3.3.1.
[589] The Norwegian Health Research Act section 6; and Regulation on the organization of health research (FOR-2009-07-01-955).
[590] Ibid.
[591] The Norwegian Health Research Act sections 10 and 33.
[592] Ibid. section 2.
[593] Ibid section 14; and Juridika, legal comments, the Norwegian Health Register Act section 2 e).
[594] The Norwegian Act concerning the Organization of Work on Ethics and Integrity in Research of 28 April 2017 (The Norwegian Research Ethics Act) section 1.
[595] Ibid. section 5.
[596] The Norwegian Regulation relating to clinical trials on medicinal products for human use (FOR-2009-10-30-1321) (The Norwegian Regulation on clinical trials).

Clinical trials require prior approval from REC. In addition, an application for an authorization of a Clinical Trial must be sent to the Norwegian Medicines Agency.[597]

As a main rule, participation of research subjects requires their informed consent. The same rule applies for the processing of health data. A consent may always be withdrawn. However, please note that a withdrawal will not affect already processed data, which will continue being part of the study.[598]

11.7 Access to health data for secondary use

11.7.1 Access to health data in medical records

General

All public and private entities offering health care are obliged to keep medical records to perform, administrate or ensure health care to individuals. Processing of health data in medical records is regulated by the Health Records Act.[599] If provided by law, medical records may be accessed for other purposes than to provide health care to individuals.[600] Such processing are subject to the requirements of the GDPR.

At the time of this report, each citizen of Norway has more than one medical record. An individual's health data is spread between public and private health care providers, primary and specialist care services, and the different health regions.

However, there is an ongoing project to collate all health data regarding an individual into one common portal. The project is called the 'one patient, one journal' project.[601] As a result, individuals will have secure access to own personal health data through an electronic portal called Min Helse[602] ("My health").[603] Further, the Directorate on ehealth is working towards providing a national electronic medical record for all primary and municipal health services.[604] The project is called Akson.[605] Akson also aims at strengthening the cooperation between different actors in the health sector by increasing access to health data within primary and municipal health services.

Health care personnel providing health care to a person have the right access this person's medical records, including medical records kept by other health care providers.[606] How the access is organized must be considered by the data controller and could include message exchange, access, copying considering the purpose of disclosure, information security, resources, infrastructure, etc. A general requirement is that the patient's right to necessary health care, the professional secrecy and the patients' requirements for confidentiality must be complied with.[607] The person may restrict the access.

Data subjects may request a copy of their health data and other personal data. The copies can be shared with innovators.

The data subject's consent and access to own medical records as a basis for secondary use

The data subject has a right to access own medical record and summary care record.[608] Access by others can be based on consent from the data subject.[609] The data subject has a right to receive a copy of its own medical record.[610] There are no restrictions on use of such copies. Thus, the data subject can decide to share the copies with anyone, including innovators.

In general, there are no restrictions on what secondary use purposes health data can be used for provided consent is obtained. Patients have a right to oppose to transfer of and access to own medical records.[611] Insurance companies are denied access such data regardless of the data subject's consent.[612]

Medical records of deceased persons may as a rule be accessed by the person's close relatives.[613]

Access to medical records for research purposes

According to the Health Research Act, REC can approve use of health data from medical records for secondary use purposes, this includes medical records of deceased persons. The authority includes access for the purpose of

[597] The Norwegian regulation on clinical trials section 1-10, cf. chapters 3 (REC) and 4 (the Norwegian Medicines Agency)
[598] Ibid. section 2-3.
[599] The Norwegian Act on Health Records of 20 June 2014 (The Norwegian Health Records Act).
[600] The Norwegian Health Records Act section 20.
[601] Meld. St. 9 Én innbygger – én journal.
[602] Helse Norge, https://minhelse.helsenorge.no/
[603] At the time of this report, persons based in the health regions of north, west and south east (Helse Nord, Helse Sør-Øst og Helse Vest) have access to Min Helse.
[604] Municipal Health Services means that all publicly organized health care services that do not belong to state or county authorities cf. the Norwegian Health and Care Services Act.
[605] Sentralt styringsdokument Akson: Helhetlig samhandling og felles kommunal journalløsning, Directorate on Ehealth, IE-1056 (2020): https://ehelse.no/publikasjoner/sentralt-styringsdokument-akson-helhetlig-samhandling-og-felles-kommunal-journallosning/Sentralt%20styringsdokument%20Akson%20Helhetlig%20samhandling%20og%20felles%20kommunal%20journall%C3%B8sning%20(PDF).pdf
[606] The Norwegian Health Personnel Act section 45.
[607] Norwegian Directorate of Health, Helsepersonelloven med kommentarer (Circular on the NorwegianHealth Personnel Act, published 28.06.2018)
[608] The Norwegian Patient and User Rights Act of 2 July 1999 (The Norwegian Patient and User Rights Act) section 5-1 and the Regulation on the Summary Care Record section 6
[609] The Norwegian Patient and User Rights Act section 3-6 and the Norwegian Health personnel Act section 22.
[610] The Norwegian Patient and User Rights Act section 5 and the GDPR article 15.
[611] The Norwegian Patient and User Rights Act section 5-3.
[612] The Norwegian Health Personnel Act section 22, first paragraph, second punctuation.
[613] The Norwegian Patient and User Rights Act section 3-3 (3).

health and medical research as described above, as well as other types of research.[614] If innovation activities can be characterized as health and medical research within the scope of the act, access can also be granted for this purpose. However, as there is no definition of the term research in the act[615], it is difficult to assess the exact scope of REC's authority in this regard and whether access may be granted for innovation activities in a wider sense.

Access to medical records for quality assurance and health data analyses

Health data may be accessed for the purposes of health analyzes and quality assurance, administration, planning, or management of the health care administration to improve health services across organizations.[616]

Quality assurance includes projects, surveys and evaluations that aim at verifying that diagnostics and treatments produce the intended results.[617] Health analyzes includes description and analysis of the prevalence of diseases and injuries in the population, and distribution of risk factors in different population groups.[618] For innovation activities regarded as quality assurance and health analyzes in this sense, access to health data from medical records may be permitted.

Access is dependent on a dispensation from the duty of professional secrecy from the Health Directorate. The dispensation may be given only if the processing is deemed to be of significant interest to the society, and the patient's integrity and welfare is sufficiently considered.[619] Personal data should mainly be disclosed in a non-identifiable format. Use of direct identifiable personal data, such as name or national identity number, is only allowed in special cases.

Innovators may access to health data from medical records for health analyzes and quality assurance.

11.7.2 Access to health data in national health registries

General

Norway has more than 100 health registries, including several comprehensive national health registries, smaller quality registries and population-based health surveys. Establishment of such health registries in the health administration and the health care sector is regulated by the Health Register Act.[620] The act regulates secondary use and applies to processing of health data for the purposes of statistics, health analysis, research, planning, preparedness, steering and quality management in the public health administration, and public health services - all different types of secondary use. Establishment of such registries must comply with the GDPR and any specific requirements set out in the Health Register Act. All processing of health data regulated by this act, also health data of deceased persons[621], is subject to professional secrecy, thus access to health data are depended on the data subject's consent or, any exemption in legislation waiving the professional secrecy as a dispensation from an adequate authority.

The data should primarily be disclosed in a non-identifiable format.

Secondary use of health data from national health registries

The registries have different data controllers, for example the Norwegian Institute of Public Health, the Cancer Registry, and the Directorate of Health. For each register there is a separate regulation which provide detailed rules on data access.[622] Access may be granted when within the purpose of the relevant register and the data controllers have a legal basis to disclose the health data in question, e.g. consent, dispensation from the professional secrecy or an alternative legal basis as provided for in the GDPR.[623] To access health data from any of these health registries, an application must be sent to the relevant data controller.

- Indirectly identifiable personal data: Indirectly identifiable personal data may be disclosed without the data subject's consent and a dispensation from the duty of professional secrecy i.e. for the purposes of health analyses, quality assurance or scientific research. Such disclosure must be of substantial value to the society, in line with ethical principles, and in consideration of the data subject's right to confidentiality and integrity.624
- Compiled data sets: Compiled data sets from different health registers may be disclosed to third parties within the purposes of the Health Register Act provided the data sets are indirectly identifiable625

[614] The Norwegian Health Personnel Act section 29 and the Norwegian Health Research Act section 35. REC is delegated this authority from the ministry of Health and Care services, cf. FOR-2009-07-02-989.
[615] Circular on the Health Personnel Act.
[616] The Norwegian Health Personnel Act section 29b.
[617] Prop.23 L (2009–2010) Amendments of the Health Register Act and the Health Personnel Act.
[618] Prop. 72 L. (2013-2014) The Health Records Act and the Health Register Act.
[619] The Norwegian Health Personnel Act section 29b.
[620] The Norwegian Health Register Act.
[621] Ibid. section 3.
[622] Prop. 63 L (2019–2020) new sections 19 and 19 a-h includes a proposal to amend the act, so the rights of access are defined in the act directly
[623] cf. the Health Register Act section 6 and the GDPR article 6 and 9.
[624] The Norwegian Health Register Act section 20.
[625] L.c.

and a legal basis in the GDPR626, hereunder either consent or a dispensation from the duty of professional secrecy.627

When data from several registries is required, separate applications for access must be submitted to the respective data controllers. As from December 2019, applications to access registries controlled by FHI, The Health Directorate, and The Cancer Registry are processed by Helsedataservice and only one application form is required.[628] Although access approval from different data controllers may be required, one need only one dispensation from the duty of professional secrecy.

Statistics and other anonymous data may in principle be disclosed and used freely. Despite this, one must apply for access.

Access for scientific research purposes need an additional approval from REC, cf. this report section 11.6.2.

In principle, statistics and other anonymous data may be disclosed and used for any purpose. However, access must be applied for.[629]

Secondary use of health Data from national medical quality registries

A medical quality registry is a health registry where continuous results from health care are documented for a limited patient group based on their individual treatment.[630] The registries may also include socio-economic, demographic and patient-reported information.[631]

As a main rule, processing of personal data in these registries are based on the data subject's consent.[632] Approval of an application to access health data in a Medical Quality registry may be granted anyone, including innovators established outside Norway for improvement of health care services through statistics, analyses and research, provided such access is:

- based on the data subject's consent; or
- based on a dispensation from the professional secrecy; and
- based on a legal basis in the GDPR, provided limited possibility of personal identification; or
- to anonymous data only, as such data may be disclosed and used freely.

Health data in medical quality registries can be compiled with data in health registries established in accordance with the Health Registry Act or the National Population Registry, and Socio-economic data in other public registries.[633]

Secondary use of health data from population-based health surveys

Population- based health surveys are performed through examination of the health conditions of the whole population, population groups, or representative samples of the population. Such surveys contain health data and possibly biological human material. Access to the material and related data is regulated by the Health Register Act.[634]

The surveys are based on the consent of the participants and collected data can be disclosed within the scope of the consent and the purpose of the survey. If the scope of consent meets the purpose of the survey, access to collected health data may be granted. The amount of personal identification included in disclosed data should be limited to what is considered necessary for the purpose of disclosure.

Access to data in health registers may be provided after an assessment from the data controller.

The data subject's consent or a dispensation from professional secrecy is also required.

11.7.3 Access to health data in the health administration

General

In addition to health care personnel, health data maybe processed by, inter alia, by other personnel within the specialist health services, the municipality health services, and the public administration in general.

Personnel in the municipality health care services[635] and in the specialist health service[636] are subject to a duty of professional secrecy applicable to the public administration. Due to this duty, such personnel cannot

626 Pluss a supplementary legal basis.
627 Ot.prop. 56 LS chapter 38.2.
628 Helsedata, Access to personal data, https://helsedata.no/soknadshjelp-personidentifiserbare/
629 Helsedata, Access to aggregated data, https://helsedata.no/soknadshjelp-aggregerte-opplysninger/
630 The Regulation on Medical Quality Registries (FOR-2019-06-21-789) (the Regulation on medical quality registries) section 1-1.
631 National Quality Registries are established based on the Health Register Act section 6 and the Regulation on medical quality registries.
632 Regulation on medical quality registries section 3-1.
633 Ibid. section 4-2.
634 The processing of personal data in Population based Health Surveys is established based on the Health Registry Act section 9 and regulated in the regulation on population-based health surveys (FOR-2018-04-27-645) section 4-1.
635 The Norwegian Health and Care Services Act section 12-1
636 The Norwegian Specialists Health Service Act section 6-1.

provide access to any information regarding someone's personal affairs. [637] The term "personal affairs" includes information about family and relative relations, internal emotional life, and physical and mental health.[638]

Secondary use

Similar as the duty of professional secrecy under the health legislation, the duty of professional secrecy for non-health care personnel can be waived by the data subject's consent.[639] Furthermore, health data collected within the health service can be used for scientific research purposes, provided a dispensation from REC, as described in this report section 11.7.1 , is obtained.[640] In these circumstances, data subject's consent is not required.

The term 'research' is not defined in the Public Administrative Act.[641] However, the preparatory works for the Public Administration Act appears to indicate that the research in question must be connected to a legitimate research institution.[642] There is no mention of innovation activities in the act, nor the preparatory works.

11.7.4 Access to health data in biobanks

General

There are two national biobanks containing human biological material in Norway, a clinical biobank for treatments, and a population-based biobank for research. There is also a biobank registry containing information regarding existing biobanks.[643]

Treatment biobanks are mainly established for primary use purposes and are regulated by the Treatment Biobank Act.[644] The act does not apply to human biological material, nor health and personal data deriving from human biological material either used or intended to be used in research.[645] Such material will be contained in a research biobank regulated by the Health Research Act.

Secondary use of biological material in treatment biobanks

Without the data subject's consent, REC may approve use of biological material collected by health care personnel or the health service for scientific research purposes.[646] Access for innovation is not mentioned explicitly.

Secondary use of health data originating from research biobanks

As mentioned above, research biobanks are mainly established for secondary use purposes and are regulated by the Health Research Act. To establish a research biobank, prior approval from REC is required. A condition for approval is that the research biobank is managed by a responsible person with a degree in medicine or biology.[647]

Further use of the material and data is dependent on an approval from REC, which only will be given "if the research in question is of significant interest to society, and the participants' welfare and integrity are ensured".[648]

For other researchers, access to material in research biobanks can be granted by the person or body responsible for the research, provided the necessary approvals from REC are contained.[649] Health data may be accessed and further processed based on a consent or dispensation from REC, stating that the duty of professional secrecy is disregarded. Please refer to this report section 11.6.2.[650] Processing must also comply with the GDPR.

Transfer of health data or biological material outside Norway

Transfer of a treatment biobank, partly or in whole, outside Norway, the transfer must be approved by the National Institute of Public Health and be in accordance with the consent of the donor.[651] The Directorate of Health may also provide a general permission regarding transfer of biobank material abroad when considered necessary to participate in international cooperation.[652]

Health data derived from biological material can be transferred outside Norway when a Norwegian researcher participate in an international research project. In such cases, anonymization or de-identification of the data in question is required.[653]

---

[637] The Norwegian Act relating to procedure in cases concerning the public administration of 10 February 1967 (the Norwegian Public Administration Act) section 13.
[638] Ot. prp. nr. 3 (1976-1977) p. 14.
[639] Ibid. section 13a (1).
[640] Ibid. section 13 d.
[641] Circular on the Norwegian Health Personnel Act.
[642] Ot.prp.nr.3 (1976-1977) s. 47-52.
[643] The Biobank Registry, https://biobankregisteret.no
[644] The Norwegian Act relating to treatment Biobanks of 21 February 2003 (the Norwegian Treatment Biobank Act).
[645] The Norwegian Treatment Biobank Act sections 3 and 5.
[646] The Norwegian Health Research Act section 28 and the Norwegian Treatment Biobank Act sections 13 and 15.
[647] The Norwegian Health Research Act sections 25 and 26.
[648] Ibid. section 28.
[649] Ibid. section 31 cf. section 4 e).
[650] Ibid. section 35.
[651] The Norwegian Treatment Biobank Act section 10.
[652] The Regulation on transfer of biobank material abroad (FOR-2004-02-26-511) section 7.
[653] Ibid. section 4.

11.7.5 Access to health data in national archives

General

The Norwegian Health Archives (Norsk Helsearkiv) was established in 2019. It is established pursuant to the Health Registry Act and the Archives Act, and is regulated by the Health Archive Regulation.[654] The purpose of the register is to preserve older, valuable medical records from the specialist health services and make the information available to researchers and others in accordance with existing regulations on the duty of professional secrecy.[655] Health data can also be found in other parts of the National Archives.[656]

Secondary use

Health data in the National Archives can be accessed and used upon their permission, provided accordance with the duty of professional secrecy applicable to health care personnel.[657]

As the general rule, data for scientific research purposes shall be made available without any direct or indirect identifiable characteristics. If direct personally identifiable characteristics are considered necessary, information may be disclosed upon approval of REC.[658] The rule applies for any health data stored in the archive.

Anyone, including innovators, may access data in the archive, provided accordance with applicable professional secrecy.[659] As mentioned in this report section 11.6.3, confidential information may be used for research purposes.[660] According to the guidelines for the National Archives, individuals requesting access for research purposes must have enough professional expertise to complete the research project. In addition, the National Archive appear to require that the individual holds a scientific position which may constitute an obstacle to SMEs.[661]

11.7.6 Access to health data in Statistics Norway

General

Since 1973, Statistics Norway has collected data on health and living conditions on a regular basis. Thus, Statistics Norway is a valuable data source for describing trends in the population.[662]

Identifiable data processed by Statistics Norway is subject to professional secrecy.[663] Thus, as a starting point, unauthorized persons cannot access data regarding individuals' personal affairs. The term 'personal affairs' should be understood in the same way as in the Public Administration Act, and includes information about family and relative relations, internal emotional life, and physical and mental health.

At the time of this report, Statistics Norway is regulated partly by the existing Statistics Act, and partly by the provisions of the new Statistics Act that have entered into force. The new act is expected to enter into force in its entirety on 1 January 2021. Any variations between the two acts will be addressed in the following.

Secondary use

The Norwegian Data Protection Authority (the Norwegian DPA) hold the authority to disregard the duty of professional secrecy. Upon implementation of the new act, Statistics Norway will hold this authority. The duty of professional secrecy can be disregarded for the preparation of official statistics or for other use, such as research.[664] Neither the existing act nor the new act includes any definition of the term 'research'. Presumably, the term is understood equivalent as in the Public Administration Act and refers to research activity connected to a legitimate research institution.

Only research institutions and public authorities are allowed access to health data.[665] It is emphasized in the preparatory works for the new act that due to the sensitive character of health data stored in registers, non-research institutions and non-public authorities shall not be granted access to such data. In addition, Statistics Norway does not hold the authority to grant access to health data received from health registries. Access to such data must be in accordance with the provisions in the Health care Personnel Act and the Health Registry Act.[666]

According to the new act, Norwegian Ministry of Finance may implement further regulations regarding access of data for secondary use. The authority is not limited to specific types of data or accessors.[667]

---

[654] The Regulation on Norwegian Health Archive and the Health Archive Registry (FOR-2016-03-18-268) (The Health Archive Regulation).
[655] Ibid. section 31.
[656] The National Archives Services consist of the National Archives, the eight regional state archives, the Sámi Archives and the Norwegian Health Archives.
[657] Ibid. sections 30 and 31.
[658] Ibid section 31.
[659] The Regulation on Public Archives (FOR-2017-12-15-2105) section 24.
[660] The Norwegian Act relating to procedure in cases concerning the public administration of 10 February 1967 (the Norwegian Public Administration Act) section 13 d).
[661] The National Archive Services, https://www.arkivverket.no/en/using-the-archives/access-to-recent-archival-material#!#block-body-3
[662] Regjeringen.no, https://www.regjeringen.no/no/tema/helse-og-omsorg/e-helse/innsikt/innsamling-av-helsedata/id2500919/, 18 May 2016.
[663] The Act relating to official statistics and Statistics Norway of 16 June 1989 (Existing Statistics Act) section 2-4 and the Act relating to official statistics and Statistics Norway of 21 June 2019 (the New Statistics Act) section 8 (not implemented).
[664] The existing Statistics Act section 2-5 cf. Ot.prp.nr.58 (1988-1989) p. 30; and the New Statistics Act section 16
[665] Only researchers, research institutions and public authorities may access the data from Statistics Norway (Prop. 72 LS 2018-2019 p. 56).
[666] Prop. 72 LS (2018-2019) p. 57.
[667] The New Statistics Act section 14 (6) (not implemented).

While the existing act does not provide grounds for free use of anonymized data without prior approval from the Data Protection Authorities[668], the new act introduces the possibility for Statistics Norway to make anonymous data publicly available.[669] However, as it is demanding to ensure complete anonymization, it is anticipated that the amount of anonymous data made available will be limited.

Statistics Norway can permit researchers access to microdata. Neither the existing nor the new act limit transfer of health data to researchers, research institutions or public authorities in Norway. However, Statistics Norway has stated that indirectly identifiable personal data (pseudonymized data) from Statistics Norway cannot be stored outside Norway. For this reason, Statistics Norway will not enter into agreements on lending of such data to foreign research institutions. In this regard, an exception is made for foreign research institution approved by Statistics Norway[670], which may access anonymous microdata.[671]

Further, for researchers outside Norway requiring access to indirectly identifiable personal data from Statistics Norway, collaboration with an approved research institution in Norway is required. It is also required that the research is conducted at an institution in Norway or via an approved remote connection, that the researchers are employed by the Norwegian research institution or have other formal connection to the institution (e.g. guest researcher), and that the researchers have signed a declaration of confidentiality.[672] In addition, due to the risk of data going astray, it is stated that institutions

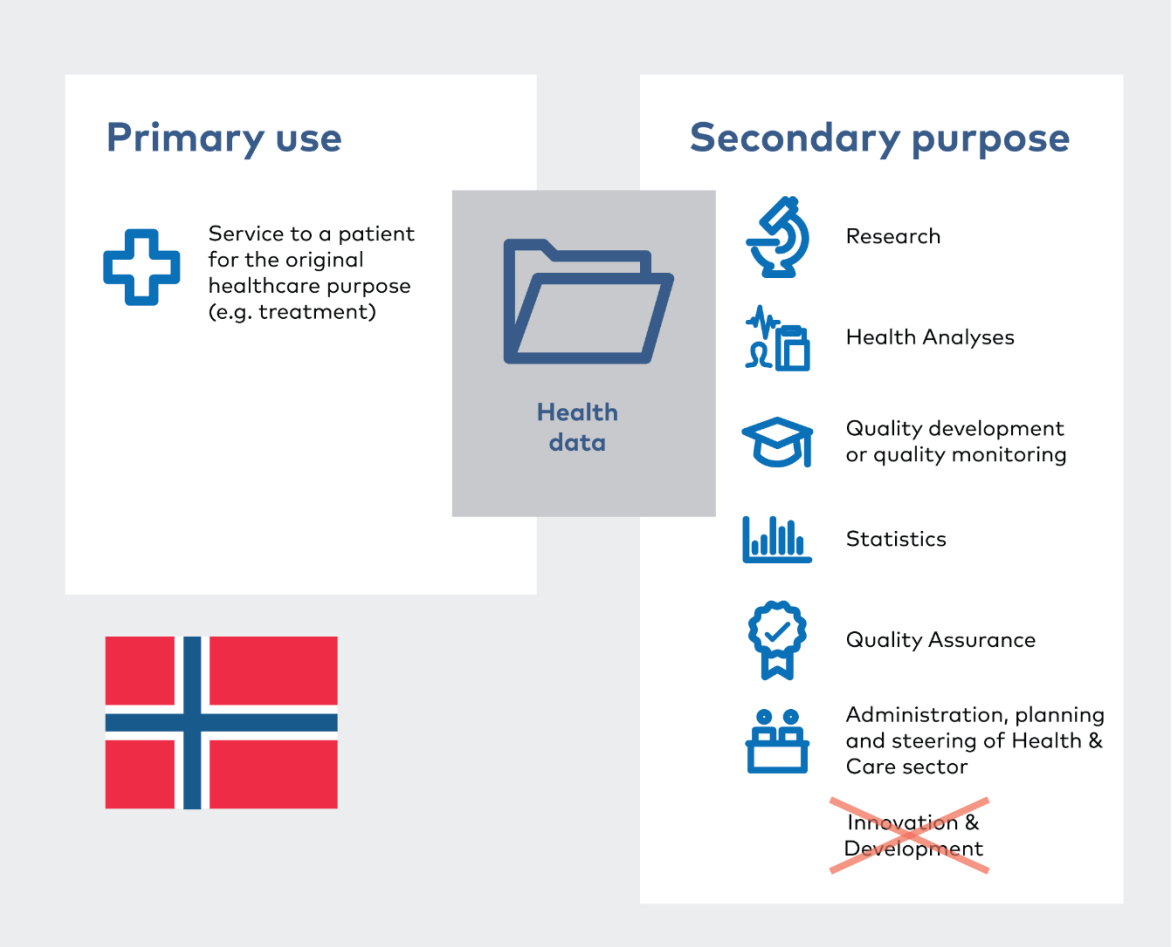


Figure 9 - Regulated division of primary and secondary use of health data in Norway

[668] This is regarded as "other use" set in the existing Statistics Act section 2-5 cf. Prop. 72 LS (2018-2019) p.63.
[669] The New Statistics Act section 15.
[670] List of approved research institutions: https://www.ssb.no/omssb/tjenester-og-verktoy/data-til-forskning/godkjente-forskningsinstitusjoner. An institution may be approved by Statistics Norway after an application, but the outset is that it must be an institution within the scope of the Act relating to Universities and University Colleges or an institution within the scope of the Public basic funding of research institutes and research groups: https://www.regjeringen.no/no/dokumenter/retningslinjer-for-statlig-grunnfinansiering-av-forskningsinstitutter-og-forskningskonsern/id2690610/
[671] Statistics Norway, *Data til forskning - steg for steg,* https://www.ssb.no/omssb/tjenester-og-verktoy/data-til-forskning.
[672] Statistics Norway, *Data til forskning - steg for steg,* https://www.ssb.no/omssb/tjenester-og-verktoy/data-til-forskning.

generally will not be given access to data for use outside of Norway.[673]

11.8 Transfer of and transborder access to health data

Transfer of personal data is in general regulated by the articles of the GDPR. The GDPR requires free movement of data within the EU, provided there is a legal basis for the transfer. The GDPR also sets forth the conditions under which data may be transferred outside the EU, cf. chapter 4.7.

There are no provisions in the health legislation that regulate or prevent the processing of health data across national borders. Hence, the transfer of health data would comply with the GDPR.

When information is to be provided to researchers, innovators or others abroad, the question of a dispensation or exemption from professional secrecy under the Health Personnel Act must be decided according to the regulations set in the Act. The fact that the Health Personnel Act applies to health personnel and companies that provide health care in Norway cannot limit the possibility that the data can be given to recipients outside Norway. The authority to make a dispensation from professional secrecy is delegated to REC and the Directorate of Health, depending on the purpose of the dispensation. This authority is not contingent on the geographical scope set in section 4 of the Health Research Act where it is stated that the act applies to data controllers established in Norway.[674]

The regulations set in existing and the New Statistics Act are neither limiting transfer of health data to researchers, research institutions or public authorities outside Norway. Nevertheless, due to the risk of data going astray, the preparatory works of the New Statistics Act have stated that institutions will as a general rule not be given access to the data for use outside of Norway.[675]

11.9 National obstacles

11.9.1 Decentralized information

In Norway, valuable health data is found in several different information resources. These information resources are regulated by different legislation, managed by different data controllers, and supervised by various public authorities.

Although there are certain exceptions from the duty of professional secrecy, access is generally dependent on the purpose of the access, as well as relevant permits and dispensation from the professional secrecy. Due to this complicated regulatory landscape, it is challenging to attain a full overview over when a permit is required, recognized purposes for obtaining such a permit, how to apply for a permit and from whom, and the relevant conditions that must be fulfilled. Lack of a fully centralized system for collection and administration of data requests further complicates the process.

11.9.2 Lack of innovation specific regulation for the secondary use of health and social data

Although there are several exemptions from the duty of professional secrecy allowing access to health data for different various purposes it is not apparent that innovation represents a legitimate purpose in this context, as innovation is not explicitly regulated in any acts and regulations for secondary use of health data.

Thus, for access to health data without the data subject's consent, the innovative activities must be characterized as research or covered by any other legitimate purpose as quality assurance or health analysis.

> *No provisions in the Norwegian legislation prevent processing of health data across national borders.*

[673] Prop. 72 LS (2018-2019) p. 56.
[674] *The Health Records Act and the Health Register Act,* Sverre Engelschiøn og Elisabeth Vigerust, Legal comments, 2. edition, 2019 p. 244, Juridika.
[675] Prop. 72 LS (2018-2019) p. 56.

12. Sweden

12.1 Introduction

Sweden has a long tradition of documenting health care provided to its citizens, and to extract this information into various information sources by which the information can be used for secondary purposes. This tradition creates an excellent opportunity for value adding re-usage of health data for various purposes.

Swedish legislation addresses the possibility to use health data collected for primary purposes for other, secondary, purposes. For example, research and quality assurance are purposes for which health data may be used under certain circumstances.[676] However, innovation as a purpose is not expressly addressed in Swedish legislation applicable to health data.

In Sweden, the field of health data is governed by a variety of acts and regulations, both on EU level and by local law. In this chapter, the Swedish health care system and health data legislation as well as the legislation governing access to documentation established within health care in Sweden will be described.

The focus is that normally, the information obtained within health care is subject to both data protection legislation, as well as legislation on public access to official documents.[677] The two legal fields are not always aligned, however, to promote re-use of health data for innovation purposes, both must be considered.

Beyond analyzing the possibilities for an innovator to access health data, the practical implications of the Swedish legislation are addressed. For an efficient secondary use of health data, the data must be easy to access and process. Hence, this chapter investigates in what forms health data may be accessed, and the process of accessing such data. For example, it is shown that the lack of centralized information sources creates obstacles in terms of time-consuming information requests to various actors, and that the existing legislation may result in innovators having a legal right to access health data, however, only in form of paper copies.

12.2 Swedish health care system and information resources

In Sweden, the responsibility for health care is divided between three different administrative levels: the government, the regions and the municipalities. The Ministry of Health and Social Affairs, a ministry in the government of Sweden, is responsible for establishing principles and guidelines along with establishing the overall political agenda for the Swedish health care. The 21 regional bodies in Sweden are primarily responsible for organizing and funding the health care to ensure good health care for all citizens. The 290 municipalities in Sweden hold the responsibility for care of the elderly and disabled, along with care of patients who have finished treatment. The Swedish health care system is mainly financed by the regional and municipality taxes, along with subsidy from the government.

Swedish legislation addresses the possibility to use health data collected for primary purposes for secondary purposes as research and quality assurance.

Innovation is not explicitly addressed as a secondary purpose.

Sweden has a long tradition of documenting health care provided to its citizens, and to extract information obtained within health care to records to be used for secondary purposes. The information sources in Sweden can be divided into primary information sources, used during providing health care to individuals, and secondary information sources, containing information from primary information sources presented and combined for secondary purposes. The main primary information source is the medical records that health care providers are obligated to keep in the provision of health care. The main secondary information sources are quality registries, health data registries and bio banks. Supplementing the secondary information sources, a selection of metadata tools and records are developed to identify what information that can be found in the various secondary information sources. An example is RUT, a tool used by researchers to better understand what specific information that is contained in certain health data registries to more precisely specify their data requests.

Significant for the health care sector in Sweden is that huge volumes of health data are processed and documented daily in various systems, also enabling secondary use. However, generally the coordination of these information sources is considered inadequate,

[676] I.e. the Swedish Patient Data Act (Swe. Patiendatalag (2008:355)) (The Swedish Patient Data Act) chapter 2, section 4 and the Swedish Act on Bio Banks (Swe. Lag om biobanker i hälso- och sjukvården m.m. (2002:297)) (The Swedish Bio Bank Act) chapter 2, section 2.

[677] Agency refers to the administrative bodies that are part of the public legal government or municipal organization.

creating challenges of overviewing and accessing available information.

12.3 Legal reforms enabling secondary use

In 2016, the Swedish Government adopted a strategy within the area of digitization of health care, called the eHealth 2025 vision[678]. The vision is that in 2025, Sweden will be world-leading in utilizing the opportunities provided by digitization and eHealth, making it easier for people to achieve good and equal health and welfare, as well as to develop and strengthen resources for increased independence and participation promoting own health.

As a starting point for reaching the eHealth 2025 vision is altering national health regulation to achieve a balance between relevant rights or interests such as protection of privacy, quality, safety and efficiency.
Regulation governing activities must guarantee the different rights and interests of the individual while at the same time address technical development.[679]

The Swedish eHealth Agency has been given the task of leading and coordinating government e-health initiatives. Further, the Swedish eHealth Agency has also been given the task with developing a long-term plan for how to administer eHealth standards in Sweden.

The Swedish eHealth Agency has pointed out how international cooperation can develop eHealth. The Agency raises the fact that in the area of international cooperation agreements, eHealth is becoming an increasingly important topic. The report encourages a closer cooperation between the countries and self governing territories in the Nordic region and suggests that this would improve the national development as well. There is already a Nordic ePrescription project in place and the hope is that this project will lead the way for cross boarder health data exchange.[680]

The government has also appointed a special committee for the inquiry "Biobanks of the future"[681], which has addressed the need of a national registry of existing biobanks to ensure national access and traceability of biobank samples, including a fit-for-purpose IT infrastructure.

Furthermore, as a part of the eHealth 2025 vision, the Swedish Government has defined a more consistent use of terminology as a national goal. Such consistency would contribute to ensuring that concepts, codes, structures and terms used are valid and usable in the work of the entities responsible. This would also enable the information exchange required to guarantee security and quality.[682]

> *Within the heath care sector, a significant volume of health data is processed and documented daily. Due to inadequate coordination of information sources, it is difficult to obtain an overview and assess available information.*

The Government has also addressed standardization as a requirement to make it technically possible to exchange information, not risking quality or security. Common technical standards are also a precondition for interoperability between different components and actors.

A national project concerning the possibilities of launching a service for gathering citizen's consent for processing operations is to be presented to the Swedish regions and municipalities during the spring of 2020.[683]
This service could also allow citizens to keep track of where and to what they have given their consent. The hope is that the project will improve care providers possibilities of sharing patient's medical records with each other, while also facilitating the individuals' consent.

12.4 Legislation

12.4.1 Data protection

In Sweden, the Data Protection Act regulates general aspects of data protection, while sector-specific data protection is governed by a variety of acts.[684] Swedish legislation contains both sector-specific data protection acts, such as the Patient Data Act,[685] as well as specific data protection provisions incorporated in other parts of the legislation, such as in the Bio Bank Act. The Data Protection Act does not apply when another data protection provision is applicable to the processing of personal data.[686]

The Data Protection Act complements the GDPR, and refers to provisions, prerequisites and definitions in the GDPR. Hence, it is not possible to interpret and apply the Data Protection Act independently from the GDPR. The Data Protection Act outlines the general provisions for processing special categories of personal data within

[678] Government Report – Vision for eHealth 2020 (S2016/01874/FS).
[679] Ibid.
[680] E-Hälsomyndigheten – Det internationella samarbetet avseende e-hälsa 2019.
[681] SOU 2018:4.
[682] Government Report – Vision for eHealth 2020 (S2016/01874/FS).
[683] Inera, https://www.inera.se/projekt/utvidgad-samtyckestjanst/
[684] The Swedish Act with complementary provisions to EUs data protection regulation (Swe. Lag med kompletterande bestämmelser till EUs dataskyddsförordning (2018:218)) (The Swedish Data Protection Act).
685 The Swedish Patient Data Act.
686 The Swedish Data Protection Act chapter 1, section 16.

health care.[687] The lawful purposes for such processing correspond with the purposes outlined in the GDPR.[688]

The Patient Data Act is the main act governing the processing of personal data within health care in Sweden. In contrast to the GDPR, the act is partly applicable to deceased individuals. The act sets forth the conditions for processing personal data and obliges care providers to keep individual medical records. Further, it outlines the conditions for processing personal data in quality registries and contains restrictions in terms of which search criteria that can be used in health care information sources. The only special category of personal data care providers can use as search criteria are health data, and the fact that a patient has been subject to compulsory or forensic mental care. Personal data relating to criminal convictions may not be used as search terms.[689] The restrictions in lawful search terms impacts the findability of health data to be used for secondary purposes, as it prohibits agencies to use variables such as genetics or biometrics when searching for and extracting data.

The act on health data registries obligates health care providers to provide a central administrative agency with data for the purpose of inter alia quality assurance of health care, and sets the conditions for the central administrative agency's processing of personal data in such registries.[690] The patient has no influence on the processing of the individual's health data and cannot consent or oppose to certain types of processing.

Another relevant act regarding processing of health data is the Bio Bank Act, which regulates the conditions for collection, storage and usage of human biological material for, inter alia, quality assurance and research purposes.

Secrecy normally applies for information obtained within health care.

Only if the information can be disclosed without damage or harm to the individual or any related party, may such information be disclosed.

12.4.2 Professional secrecy

Sweden has an extensive and complex legislation regarding access to and secrecy for files held by agencies. Generally, as nearly all health data collected for primary purposes in Sweden are kept by agencies, disclosure of

To understand the possibilities for accessing health data, the conditions for disclosure of official files is of great importance.

health data is tried under this legislation. This applies regardless of the source and purpose of the requested information. For this reason, to understand the possibilities of accessing health data it is important to understand the applicable conditions for disclosure of official files from public care. Data protection legislation, such as the GDPR, applies to the processing of the health data that may occur after the disclosure.

In Sweden, the starting point is that anyone may access any file received or drawn up by a public agency.[691] Access should only be denied when a secrecy rule applies to the information. This concept is referred to as the principle of public access to official records. The definition of *file* includes both documents, as well as records intended for automated processing.[692]

Regarding information obtained within health care, certain secrecy provisions states that secrecy normally applies. Only if the information can be disclosed without damage or harm to the individual or any related party, such information may be disclosed. [693]

The Public Access to Information and Secrecy Act does not apply to information held by private health care providers. Secrecy in such care is regulated by the Patient Safety Act, which outlines that personnel within private health care must not, without authorization, disclose information about an individual's health condition or other personal circumstances.[694] This implies that there is no general right to access information from private health care providers. Consequently, the possibilities to access health data from the private health care sector are, at least in theory, more limited than from the public sector. However, preparatory work points out that the interpretation of the secrecy obligations in both acts shall not differ essentially in practice.[695] Hence, this report does not focus on any eventual differences between the possibilities to access health data, and only briefly highlights differences when relevant.

12.4.3 General regulation on health research

The Ethical Review Act

The Ethical Review Act entered into force in 2004 with the purpose of ensuring the interests of the individual and the

[687] Ibid. chapter 3, section 5.
[688] The GDPR Article 9 (2) h).
[689] The Swedish Patient Data Act chapter 2, section 8.
[690] The Swedish Act on Health Data Registries (Swe. Lag om hälsodataregister (1998:543)) (The Health Data Registries Act).
[691] The Swedish Freedom of Press Act chapter 2, section 1.
[692] Ibid. chapter 2, section 3.
[693] The Swedish Act on Public Access to Information and Secrecy (Swe. Offentlighets- och sekretesslag (2009:400)) (The Public Access to Information and Secrecy Act) chapter 25.
[694] The Swedish Act on Patient Safety (Swe. Patientsäkerhetslag (2010:659)) (The Patient Safety Act) chapter 6, section 12.
[695] Proposition 1980/81:28 p. 23.

respect for the individual worth in research.[696] The act applies to any research carried out in Sweden and includes processing of health data. According to the Act, the definition of research includes scientifically experimental or theoretical work, or scientific studies carried out by observation, provided that the work or study is conducted to gather new knowledge. Furthermore, developmental work on scientific basis is included in the definition of research. [697]

The act includes provisions which require an ethical review of research involving living or deceased persons or biological material from humans. The review is carried out by the Swedish Ethical Review Authority and shall be based on:

- Respect for human dignity
- Human rights and fundamental freedoms
- Interests in the development of new knowledge through research

Research may only be approved when the scientific value outweighs possible health risks, safety and the personal integrity of participants. Processing of health data may only be approved when necessary for the research.

12.5 Access to health data for secondary use

12.5.1 Files held by public agencies

In Sweden, most health data obtained for primary purposes are held in files by public agencies, such as the regions or the National Board of Health and Welfare, for example in medical records and in quality registries. As stated above, anyone may request files drawn-up or received by agencies. The agency receiving such a request, is obligated to try the request without undue delay. The request is tried under the Public Access to Information and Secrecy Act, regardless of from which information source health data is requested. The same rules apply in most cases, however, non-aggregated health data from the health data registries are subject to a stricter regulation than other types of health data held by agencies. Furthermore, access to tissue samples in bio banks are tried under the Bio Bank Act, which contains other rules for disclosure than rules applicable to files.

When an agency tries whether to disclose health data or not, it assesses whether the disclosure would cause any damage or harm to the individual or any related party.[698] If that is the case, the health data may not be disclosed.

When conducting the assessment, the agencies consider the purpose of use.

The secrecy assessment shall be conducted in the perspective of the individual, and how the individual would experience a potential disclosure. If it cannot be excluded that the patient or any related person would experience a disclosure as inconvenient, information must not be disclosed. However, disclosing pseudonymized personal information is normally not considered to cause damage or harm in a way that should hinder disclosure. The agency holding the data shall, if possible, facilitate a disclosure of a pseudonymized file.[699] Secrecy does not apply to health data held by a care provider, if the patient consents to disclosure.[700]

> *When an agency assesses whether to disclose health data or not, consideration to whether the disclosure would cause any damage or harm to the individual or any related party must be taken.*

Many agencies have established formal processes for applying for health data. These processes normally include steps evaluating how the integrity of the data subject will be protected after an eventual disclose, for example by requesting the purpose of use and who will have access to the personal data. The GDPR and other data protection legislation applies to any subsequent processing of personal data disclosed by an agency.

Agencies are only obligated to provide paper copies and not electronical copies of the official records.[701] Neither are agencies obligated to compile the information it holds, and thereby create "new" files, unless such compilation can be done using routine measures. When compilating such files containing personal data, an agency must not use search terms that are unlawful according to other legislation governing the information, for example the Patient Data Act.[702] The agency is not obligated to disclose information If disclosure greatly disturbs the agency's work, for example by requiring extensive resources.[703]

There is a possibility for agencies to disclose information otherwise subject to secrecy, when such disclosure is combined with certain conditions regarding the recipient's right to use or further disclose the information.[704] This possibility may be used when the risk for damage or harm to the individual, or any related parties, does not lie with

696 The Swedish Ethical Review Act section 1.
697 Ibid. section 2.
698 The Swedish Public Access to Information and Secrecy Act chapter 25, section 1.
699 The Swedish Freedom of Press Act chapter 2, section 15.
700 The Swedish Public Access to Information and Secrecy Act chapter 12, section 2.
701 The Swedish Freedom of Press Act chapter 2, section 16.
702 Ibid. chapter 2, section 7.
703 The Swedish Public Access to Information and Secrecy Act chapter 6, section 4.
704 Ibid. chapter 10, section 15.

the recipient's access to it, but rather with subsequent use or disclosure. Potential conditions to such access is that the information may not be made publicly available, that it must be subject to certain technical or organizational security measures, or to set a due date for destruction.

12.5.2 Processing of health data in general

Access to health data for the purpose of research

According to the GDPR, scientific and historical research should not be considered a purpose incompatible with an initial purpose.[705] Hence, there is a general possibility to process health data, regardless of the source, that has originally been collected for primary purposes for research, provided that other applicable data protection requirements are met. For example, the researcher must have a legal basis for the research and be able to ensure the security of the data.[706]

Processing personal data for research purposes requires that appropriate safeguards are in place, protecting the individuals concerned.[707] The ethical review of research projects carried out under the Ethical Review Act serves as such a safeguard.[708]

The possibility to use health data from the health care sector for research is interesting from an innovation perspective, as research and innovation in some respects overlap. According to the Ethical Review Act, which enables processing of personal data in research, the definition of research includes scientifically experimental or theoretical work, or scientific studies carried out by observation, provided that the work or studies are conducted to gather new knowledge. Furthermore, developmental work on scientific basis is included in the definition of research.[709] Experimental work refers to studies aimed at proving the effect of an intervention, where a researcher controls the test conditions. Theoretical work refers to logical argumentation, for instance within mathematics or philosophy. Normally, the latter does not include test persons. Scientific studies carried out by observation refers to studies in which the relation between different variables are studied without the researcher influencing the process, for instance epidemiologic research or research carried out using surveys or registries.[710]

The application areas of the definitions should be determined on a case-by-case basis.[711] However, the key is that for an activity to be considered research it must have a scientific approach, whether by gathering new knowledge or in development work. It is the scientific approach that distinguishes research from other similar activities, such as quality assurance or performance monitoring. Science in this context refers to a process in which knowledge is systematized and structured through theory development and application of methodical work tools.[712]

Considering the definition of research, some innovation activities may be carried out based on the lawful purpose research, provided the activities has scientific approach. Relevant in this context is that a research project must only be approved if it is performed by or under the supervision of a researcher with the necessary scientific competence.[713] Thus, an academic collaboration may be required.

According to the GDPR, scientific and historical research is not considered incompatible with an initial purpose.

Hence, it is in general possible to process health data for research purposes.

When applying for health data to be used for research with a scientific purpose, most agencies require that an approval from the Swedish Ethical Review Authority is submitted with the application, as well as information about the responsible researcher and objective of the research.[714]. As each agency independently decides whether a disclosure would cause damage or harm to an individual, the process and possibilities to access health data may differ depending on the agency holding the health data.

Although agencies generally attach great importance to the ethical assessment of a research project, it should be noted that the two assessments are separate. The fact that a research project has been approved by the Swedish Ethical Review Authority does not automatically imply that the personal data requested from an agency shall be disclosed under the principle of public access.

Normally, if a researcher is granted access, the personal data disclosed is pseudonymized. An exception is when the research cannot be conducted without personal data that can be attributed to an individual. The fact that conducting research on identifiable personal data would reduce costs or be easier does not provide grounds for such access. In terms of direct access, such may only be provided the controller of the health data.[715]

705 The GDPR Article 5 (1) b).
706 Proposition 2017/18:298 p. 39.
707 The GDPR Article 89.
708 Proposition 2017/18:298 p. 84.
709 The Swedish Ethical Review Act section 2.
710 Proposition 2018/19:165 p. 16.
711 Proposition 2002/03:50 p. 91.
712 Proposition 2007/08:44 p. 19.
713 The Swedish Ethical Review Act section 13.
714 See for example forms for applying for patient data from Region Dalarna: https://websurvey.textalk.se/se/answer/survey.php?surveyID=120785&init=1&response=MTsyZWM0M2U1MjMyOTQwMTAxMzcxZDk1Mjg3OTkwMmJiZWVkMjJiMWRhOzc7Njc5NzI3OQ%3D%3D
715 The Swedish Health Data Registries Act section 8.

Innovation activities may be carried out based on the lawful purpose of research, provided the activities has a scientific approach.

Access to health data for quality assurance

Health data in medical records, quality registries and health registries, originally collected for primary purposes, may also be processed for the secondary purpose quality assurance. As innovation and quality assurance are partly overlapping purposes, the possibility to process health data under this purpose is of relevance.

The Swedish Data Protection Authority has in a supervision decision[716] investigated the meaning of the purpose according to the data protection legislation applicable to social care in Sweden.[717] In the decision, the authority concluded that a municipality's alignment of personal data from the municipality's social care with personal data from the region's health care to jointly follow-up on these services, was unlawful. The conclusion was based on the that the purpose quality assurance is limited to the municipality's own social care organization. Pursuant to this interpretation of the Health Data Act, as the allowed purpose only includes internal quality work within the organization already holding the data, it would not be possible to access health data obtained within health care for innovation purposes, unless the data subject consents.

12.5.3 Access to health data from medical records

Legal basis for access

All provision of health care in Sweden must be documented in medical records, kept for each patient individually. Each care provider keeps its own medical record concerning the individual patient. Hence, the patient does not have a gathered medical record accessible for all care providers.

The main purpose of medical records is to ensure that the patient receives adequate and safe care, as well as to serve as an information source for the patient, supervision and research.[718] Medical records must only be destroyed or made unreadable after decision from the Health and Social Care Inspectorate (*Swe*. Inspektionen för vård och omsorg).[719]

In general, health data in medical records may only be processed for primary purposes. However, it may also be processed for quality assurance and development as well as purposes relating to the administration, planning, evaluation and supervision of the health care. Also, production of statistics serves as a lawful purpose.[720] Furthermore, health data may be processed for purposes not incompatible with the ones explicitly expressed as lawful[721], for example research[722]. A patient may consent to processing of health data for other purposes than the ones otherwise lawful, which means that health data may be used for innovation if the patient consents.[723] A patient may also access own health data, unless it due to the purpose of the care or treatment is of great importance that the patient is not granted such access.[724]

As shown, innovation is not explicitly included among the lawful purposes. Thus, health data must not be used for innovation purposes without the patient's consent, unless the innovative activities are captured by any of the explicitly lawful purposes. Nevertheless, health data may be processed for innovation activities falling under the definition of research, since research is considered compatible with the lawful purposes.

In terms of access to medical records, external parties may only be granted access if it does not cause the individual or any related party damage or harm. Considering the sensitive nature of medical records, they are normally not disclosed without consent, apart from to other care providers for health care purposes, or in certain cases to the individual's relatives.[725]

In general, health data from medical records can only be used for innovation based on the patient's consent.

Access in practice

If disclosed, the agency has no obligation to provide information electronically but only in paper copies. Thus, an innovator only has a legal right to receive paper copies of medical records. However, this is considered inconvenient, as paper copies require a lot of administration to be used efficiently.

The Patient Data Act provides a solution for such cases, by enabling a care provider to grant external parties direct access to a patient's medical record, with the patient's consent. Direct access means that the patient

716 The Swedish Data Protection Authority, decision dnr-643-2015.
717 Ordinance (2001:637) on processing of personal data within social care section 12.
718 The Swedish Patient Data Act chapter 3, section 2.
719 Ibid. chapter 3, section 14.
720 Ibid. chapter 2, section 4.
721 Ibid. chapter 2, section 5.
722 According to the GDPR, research should not be considered a purpose incompatible with an initial purpose, cf. the GDPR article 5 (1) b).
723 The Swedish Patient Data Act chapter 2, section 3.
724 The Swedish Public Access to Information and Secrecy Act chapter 25, section 6.
725 Proposition 1979/80:2 s. 168 f.

itself can access its medical records without consulting the care provider, for example by logging into a web portal. However, this possibility is limited to the patient itself, or to care providers providing health care to the patient in question. When tried by the Supreme Administrative Court[726], the court found that the patient cannot with legal effect consent to a third party being granted direct access, the reason being regulation in the Patient Data Act explicitly stating that direct access to medical records can only lawfully be granted to the extent permitted by law. Hence, at the time of this report, there is no efficient way for innovators to in practice secure electronical access to medical records.

12.5.4 Access to health data in Quality registries

In Sweden, agencies within health care may establish quality registries enabling comparison of health care on a regional or national level. These registries have been kept in Sweden since the 1970's. The purpose of such registries is to systematically and continuously develop and ensure the quality of the care. Such use is regarded secondary. Information is reported by the care providers to the quality registries on a voluntary basis. However, when information has been reported, the Patient Data Act sets out conditions for processing of personal data in quality registries. Personal data must not be processed in quality registries if the data subject refuses such processing.[727]

For example, the registries can cover a patient group with a certain diagnosis or a specific medical treatment. Further, it can contain information on an individual level, such as important background factors, diagnoses, treatments and the outcome of the care which has been provided to a patient. By comparing the information entered in the registries, care providers can conclude on how to provide care successfully. Swedish registries are near complete, containing information about patient groups from all regions.

A lawful purpose of access and subsequent processing of health data in quality registries is systematic and continuous development and quality assurance of health care, conducted by external parties to produce statistics, or to conduct research within the area of health care.[728] Although health data may be disclosed from quality registries, the strict limitations in lawful purposes indicate that health data in quality registries cannot be accessed for innovation purposes explicitly. Should the intended innovation activity fall under the definition of research, there is a lawful purpose for processing.

If the agency keeping the quality register decides to disclose data for research purposes, the data disclosed should be minimized to variables relevant for the research in question. Personal identification numbers shall only in exceptional cases be disclosed, if considered absolutely necessary for the planned research. For this reason, the personal data is normally disclosed pseudonymized, with the information key being retained at the disclosing agency. The information keys are normally disposed of after three months.[729]

Access to own personal data in quality registries should always be granted, unless otherwise stated by law.[730]

12.5.5 Access to health data in health data registries

All care providers are obligated under The Health Data Registries Act to report information to national health data registries, managed by e.g. the Swedish National Board of Health and Welfare. The registries are inter alia kept to follow up, assess, and quality assure health care.[731]

The information in the registries vary depending on the purpose of the registry. Examples of health data registries are:

- The Cancer Register (Swe: Cancerregistret) which contains facts about cancer diseases diagnosed in Sweden, for example type of tumor, date of diagnosis and information about the patient from 1958 and onward;
- The Medicine Register (Swe: Läkemedelsregistret) which contains information on all prescribed medicine that has been collected by patients from pharmacies as from 2005; and
- The Patient Register (Swe: Patientregistret) which contains patient information, including diagnosis, treatment, surgery and external cause of injuries and poisoning, from all doctors' appointments within closed and specialized open medical care. The registry dates back as far as 1964.

Common for all registries is that the information reported is linked to individual personal identification numbers, and

> *Accessing health data not directly linked to an individual may be possible under existing legislation, also for innovation purposes.*

726 HFD 2017 ref. 67.
727 The Swedish Patient Data Act chapter 7, section 2.
728 Ibid. chapter 7, section 5.
729 Nationella kvalitetsregister – Vägledning och information kring utlämnande av kvalitetsregisteruppgifter för forskning version 2018-10-02.
730 The Swedish Public Access to Information and Secrecy Act chapter 12, section 1.
731 The Swedish Health Data Registries Act section 3.

that the information is reported to health registries regardless of the patient's consent.

The right for external parties to access health data in health data registries is regulated by the Public Access to Information and Secrecy Act. The secrecy is stricter than for health data from other sources, as keeping of such registries is considered statistics operations[732], to which 'absolute secrecy' applies. The absolute secrecy entails that secrecy applies, regardless of whether a disclosure would cause the individual concerned damage or harm, unless the data is to be used for research or statistics.[733] Hence, due to the strict secrecy, accessing health data from health data registries for innovation purposes is not an option, unless the intended innovation activity falls under the definition of research.

However, accessing health data that cannot be directly attributed to an individual can under certain circumstances be possible under existing legislation, including for innovation purposes. Firstly, such disclosure requires that the information may be disclosed without damage or harm to the individual or any related party, as described under this report section 12.5.1. Secondly, the information must be available in an already existing file[734], or be able to compile by using routine measures[735] and without using unlawful search terms.[736] To facilitate such requests, the National Board of Health and Welfare has a webservice where it is possible to order anonymous data presented as statistics.[737]

12.5.6 Access to health data in biobanks

Biobanks are collections of tissue samples, collected in connection to care provider's health care operations. The biobanks also contain information about the samples and sample donors, for example analysis results, diagnoses, and survey responses. Tissue samples may only be collected and used in biobanks with the donor's consent. The purposes of secondary use for which health data in biobanks may be used are specified, and include for example quality assurance, education and research.

All biobanks should be reported to the Health and Social Care Inspectorate within a month after a decision to establish a biobank has been taken.[738] The Inspectorate keeps an automated record of biobanks[739], which, at the time of this report, consists of around 450 biobanks. A biobank or part of such can only be transferred after permission from the Health and Social Care Inspectorate. Such permission can only be granted under special circumstances, and never to a recipient outside Sweden.[740] Tissue samples stored in a biobank must never be disposed of or disclosed for commercial gain.[741]

Apart from disclosure to researchers outside Sweden, there are no general rules in the Biobank Act on when tissue samples shall or may be disclosed. However, some guidance can be found in the Biobank Act For example, the act outlines that medical records relating to a sample donor may be disclosed if the sample donor consents.[742] There is also a general provision that tissue samples shall be anonymized or coded prior to any disclosure. The code keys shall in these cases be securely stored at the care provider that decided to collect and store the tissue samples in a biobank.[743]

Tissue samples, with the sample donor's consent, may be collected and stored for research purposes.[744] Third parties access to tissue samples requires that the research project is tried by the Swedish Ethical Review Authority, which decision shall serve as guidance in the decision whether to disclose or not.[745] The sample donor must consent to the specific purpose, and it should be ensured that there is enough tissue sample remaining after disclosure to be used for diagnostic, care, and treatment of the sample donor. A biobank agreement must also be concluded with the responsible for the biobank, regulating for example how the samples may be used and for how long.[746] Preparatory works state that the possibility to disclose information for research purposes shall be very restrictively applied.[747]

12.5.7 Access to health data in municipal and state archives

Files drawn up or received by agencies, state agencies, or municipal agencies form the agencies' archives. The archives shall be preserved, kept, organized, and maintained in a way that ensures inter alia the right to access official documents.[748]

Health data stored in municipal and state archives, like health data stored by any agency, are subject to a default secrecy. Only if health data can be disclosed without damage or harm to the individual or any related party,

732 RÅ 2004:9.
733 The Swedish Public Access to Information and Secrecy Act chapter 24, section 8.
734 The Swedish Freedom of the Press Act chapter 2, section 3.
735 Ibid. chapter 2, section 6.
736 Ibid. chapter 2, section 7. Lawful search terms are information needed for the purposes of producing statistics, follow up on, assess and quality assure the health care and research and epidemiological investigations.
737 The National Board of Health and Welfare's access service: https://bestalladata.socialstyrelsen.se/statistik/
738 The Swedish Bio Bank Act chapter 2, section 5.
739 Ibid. chapter 2, section 6.
740 The Swedish Bio Bank Act chapter 4, section 7.
741 Ibid. chapter 4, section 8.
742 Ibid. chapter 4, section 4.
743 Ibid. chapter 4, section 4a.
744 Ibid. chapter 2, section 2.
745 Proposition 2001/02:44 p. 48.
746 Regionernas gemensamma biobanksdokumentation, document K1a, https://biobanksverige.se/wp-content/uploads/k1a-principer-for-tillgang-till-biobanksprov.pdf
747 Proposition 1994/95:200 s. 38.
748 The Swedish Act on Archives (Swe. Arkivlag (1990:782)) (The Swedish Archives Act) section 3.

disclosure is lawful. However, secrecy generally only applies to information about individuals for 70 years. After this time, the information may be disclosed to anyone requesting it.

12.5.8 Access to health data in Statistics Sweden

According to the Act on Official Statistics several actors, such as companies and regions, are obligated to report information to agencies responsible for statistics. At the time of this report, there are 28 agencies in Sweden responsible for statistics in different fields. The main agency, administrating most official statistics, is the Statistics Sweden (*Sw. Statistiska centralbyrån -SCB*).

As for health data registries, health data from Statistics Sweden is subject to a stricter secrecy than health data kept by most other sources. Unless the individual consents, it may only be disclosed if it is needed for research or statistics purposes, or in an anonymized form. It is in these cases furthermore required that disclosure does not cause the concerned individual any damage or harm.

For agency held health data, foreign companies may in principle access on similar premises as national companies.

12.6 Transfer of and transborder access to health data

Regarding health data held by agencies, in principle Swedish and foreign agencies can access health data on the same premise.[749] However, according to the Public Access to Information and Secrecy Act, information subject to secrecy may not be disclosed to foreign agencies unless such disclosure is in accordance with certain legal provisions, or if the information could be disclosed lawfully to a Swedish agency, and it is clear that such disclosure is in accordance with the national interests of Sweden.[750]

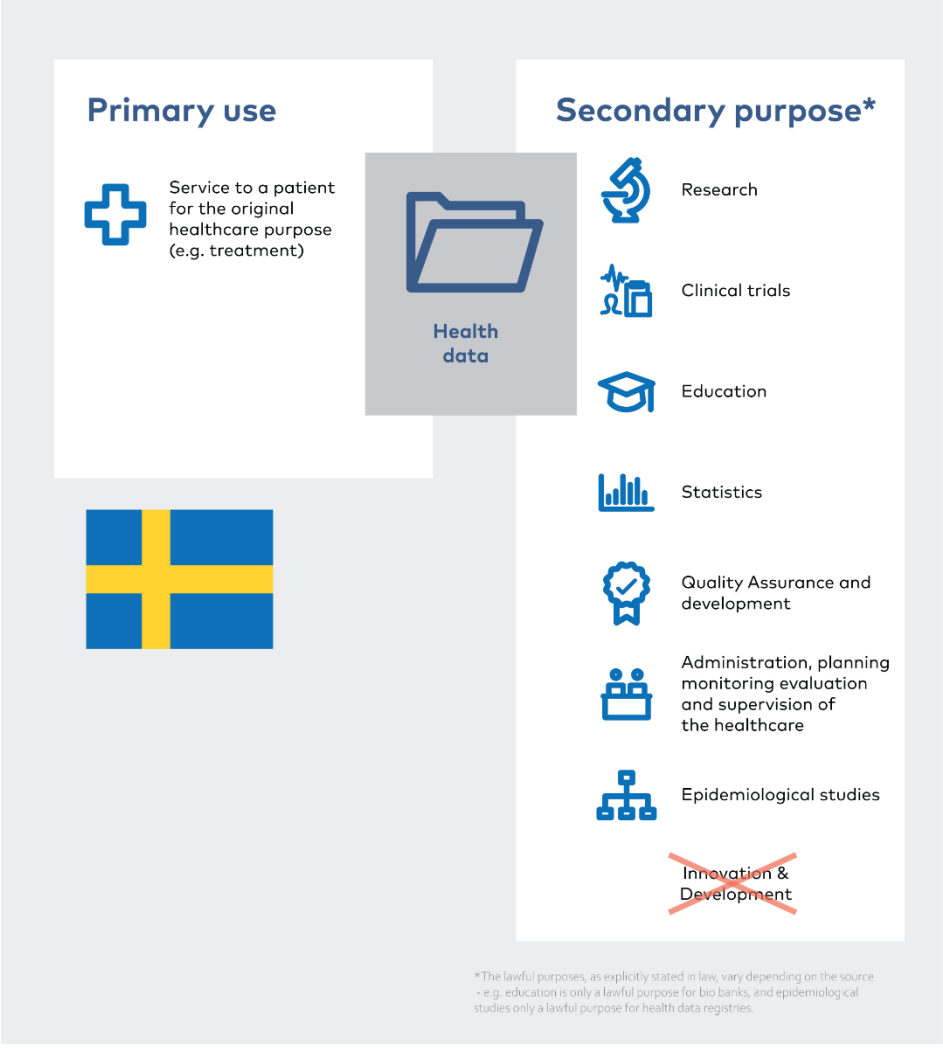


Figure 10 - Regulated division of primary and secondary use of health data in Sweden

[749] The Swedish Act on Freedom of the Press chapter 15, section 5.

750 The Swedish Public Access to Information and Secrecy Act chapter 8, section 3.

The Bio Bank Act further states that tissue samples in biobanks may not be disclosed to recipients outside Sweden, unless for conducting research. In such circumstances, a disclosure application from a Swedish research institute is required.[751]

12.7 National obstacles

12.7.1 Lack of innovation specific regulation

To lawfully collect and process health data there must always be a purpose. The Patient Data Act defines the lawful purposes for processing of health data in medical records and quality registries. Innovation and development are not amongst the listed purposes, and it is challenging to assess whether innovation and development can be regarded encompassed by the listed lawful purposes.[752] Evidently, health data obtained upon provision of health care may not be processed for innovation purposes, whether collected in medical records nor other main health data sources in Sweden, except with the data subject's consent. From an innovator's perspective, obtaining such consent introduces certain challenges. Please refer to section 13.2.1 for details on these challenges.

12.7.2 Strict secrecy rules are not aligned with Data Protection Legislation

Regardless of whether the intended processing of health data is in accordance with the data protection legislation, the health data cannot be disclosed to external parties without a secrecy assessment. Secrecy applies unless the information can be disclosed without damage or harm to the individual or any related party. In theory, the secrecy assessment is separate from the disclosure assessment under the data protection legislation. However, the relation between the secrecy assessment under the Public Access to Information and Secrecy Act, and data protection legislation is complex and not fully clarified under Swedish law. The dual assessment system complicates the process of accessing and processing health data.

12.7.3 Limitations in lawful search criteria

Although health data is a permitted as a search criterion, Swedish legislation limits the use of special categories of personal data as search criteria in registries.[753] Other special categories of personal data, such as genetic or data relating to criminal convictions may not be used as search criteria. This may impede the identification and extraction of health data from available sources, ultimately limiting the possibility of conducting innovation and development activities.

12.7.4 Limitations in medical record sharing

For different care providers, it is possible to share electronical medical record systems and thereby give each other access to personal data processed for maintaining medical records, documentation, patient care, and patient administration.[754] The patient may refuse to having its health data shared in such system.[755] A care provider may only process personal data made available in such system by another care provider for the purposes of preventing, examining and treating diseases and injuries or for issuing a care certificate. The patient cannot consent to any further processing. When tried by the Supreme Administrative Court[756], the court found that the patient may not with legal effect consent to a third party being granted direct access to the its medical record. Consequently, external parties must request the medical record from the care provider in question to receive a copy.

12.7.5 Decentralized information

Large volumes of health data are collected and documented daily. However, in practice, access to health data is limited due to lack of a common information infrastructure. The health data is spread over several sources and the legal possibilities to access the data vary between different information sources. In addition, a disclosure request must often be assessed by the agency holding the data. Thus, anyone requesting disclosure of health data will have to turn to separate agencies depending on what data they are requesting, all conducting separate assessments. Regardless of several initiatives to establish centralized systems, no such system exists at the time of this report. This significantly complexifies the process of accessing necessary health data for innovation and development purposes.

751 The Swedish Bio Bank Act chapter 4, section 3.
752 Cf. the GDPR article 6 (4)
753 Patient Data Act chapter 2, section 8.
754 Patient Data Act chapter 6, section 1.
755 The Swedish Patient Data Act chapter 6, section 2-4.
756 HFD 2017 ref. 67.

13. Use of health data across the Nordics

13.1 General

As mentioned in the introductory chapters, there are significant societal similarities between the Nordic countries and self governing territories. The spirit of voluntary communal work and the citizens reliance in the authorities are prominent features, and the Nordics have a long tradition for governmental co-operation, also in respect to legislative changes. The country specific chapters support this view, and shows that the Nordic region has shared values, similar legislative framework, and overall well establish health data and registers. Further, the chapters show that existing legislation on secondary use of health data is consistently strict throughout the Nordic region. The reason for this strict regulation can be found in the obligation in the GDPR and national health legislation to treat health data for private individuals with great cautiousness. As health data is considered as a special category of personal data, it is shielded by privacy considerations and regulations on professional secrecy. Thus, access to and processing of such data is mainly permitted upon the data subject's consent or on an alternative legal basis. In the following, legal possibilities to access and process health data under existing Nordic legislation will be emphasized. Further, obstacles that must be addressed to facilitate for innovation and development activities will be described.

13.2 Possibilities under existing legislation

13.2.1 Consent as legal basis

As mentioned above, consent is considered a legal basis for processing health data under the GDPR, as well as under the Faroese and Greenlandic data protection legislation. Consent is regarded a core principle of data protection law and an accessible legal basis for processing activities, including processing of health data for innovation and development purposes. When data subjects are involved in development processes consent should be the legal basis of choice. By obtaining consent, professional secrecy can be disregarded. For processing of health data for scientific research purposes, principles of research ethics also apply, in which the data subjects' consent can be required explicitly.

Although consent should be the legal basis of choice for processing of health data, it introduces certain challenges. Reliance on consent can be both cumbersome and inconvenient. Obtaining consent from each data subject may in many cases be a time-consuming process and it can be challenging to obtain consent from enough users willing to make their health data accessible for innovation purposes, which can result in few respondents and unrepresentative data sets. Further, several conditions must be complied with.

Firstly, the consent must be given freely, informed, and appropriately limited to the purpose of use. A challenge in this regard is to define a purpose of use precise enough to meet the level of detail required by e.g. the GDPR, without overly narrowing the scope. Deloitte Legal has received feedback from industry participants stating that they find it difficult to use consent as legal basis for processing of health data for innovation purposes. The main challenge being to prepare a precise enough purpose of use, as innovation projects often evolve quickly and change during the project. Thus, new consents from all data subjects reflecting the changes outside the original purpose of use may be required. A possible solution to this challenge can be found in that the GDPR recognizes use of broad consents in scientific research. Through using broad consents, data subjects may allow personal information to be used for certain categories of scientific research.[757] However, it has been underlined by the European Data Protection Board that when processing health data or other special categories of personal data the broad consent shall be subject to strict interpretation.[758]

Secondly, the consent must be documentable and possible to withdraw at any time in a simple and accessible way. Certain practical considerations must also be taken into consideration, such as methods for collection, procedures for review and withdrawal of consent, as well as how to secure and demonstrate compliance with the scope of consent. Due to the close relation between a patient and a health care provider, a freely given consent can be problematic to obtain.

The risk of consent withdrawal introduces additional challenges. Unless there is another legal basis for further processing, upon withdrawal the processing of health data shall discontinue, and the health data must either be deleted or anonymized. The risk of consents being withdrawn can significantly impact research or innovation projects, as it represents uncertainties regarding whether specific health data can be processed throughout the project, or if important data is required to be deleted resulting in limited and deficient data sets.

In Denmark and the Faroe Islands, the one-year limitation on a given consent represents further challenges.[759]

[757] The GDPR recital 33.
[758] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679.
[759] Cf. e.g. the Danish Health Act section 44 (2), and the Faroese Health Act section 44 (2).

Renewal of consents can be problematic to obtain, and upon lapse of consent, health data can no longer be used.

13.2.2 Alternative legal bases for secondary use of health data

Finland is the only country where innovation and development explicitly is addressed as a lawful purpose for access to health data. This is done through the newly introduced Finnish Act on the Secondary Use of Health and Social Data, one of the objectives being to facilitate for innovation and development activities. However, as health and social data can only be obtained in form of aggregated statistics for development and innovation purposes, the variability and usability of available data is somewhat limited. Thus, for access to non-anonymized data, innovators must rely on an alternative legal basis for secondary use of health data under national legislation.

In the other countries and self governing territories in the Nordic region, innovation and development are not explicitly recognized as lawful purposes for secondary use of health data. As in Finland for access to non-anonymized data, innovators must rely on an alternative legal basis for secondary use of health data under national legislation. Whether an alternative legal basis is applicable must be assessed on a case-to-case basis.

An alternative legal basis for access to and subsequent processing of health data can be found in the listed lawful purposes in national legislation, provided in accordance with the GDPR. The country specific chapters show that scientific research, health analysis, and quality assurance, among others, are recognized as lawful purposes for secondary use of health data across the Nordics. Due to the similarities between research and innovation, the national exceptions applicable for scientific research appear as the most relevant alternative legal bases.

For access to health data based on the exceptions applicable to scientific research, in addition to the conditions listed under the GDPR, the conditions listed under the relevant national law must be fulfilled. In addition, prior approval from relevant authorities or agencies are often required. Such authorities or agencies may also set separate terms for processing of data. For an accessor, it is therefore important to carefully consider the specific conditions and procedures under the applicable regulation.

For example, in Denmark, a prerequisite for access permission is that the project in question can be characterized as a research project in accordance with the Danish Committee Act, meaning that projects considered innovation or development are denied access permission. Due to lack of any specific definition being included in the legislation, the relevant authorities, typically the ethics committees, are given a certain level of freedom of assessment in this regard. Further, in Norway, innovation activities can be characterized as scientific research within the scope of the Health Research Act, provided the activities are systematic and existing knowledge from research and practical experience is applied to improve existing products, processes, systems, and services. If these conditions are fulfilled, REC may allow access to relevant data. The situation is similar in Sweden, Iceland, the Faroe Islands, and Greenland.

The main challenge connected to alternative legal bases is to determine the area of application. Please refer to section 13.3.1 for details on this challenge.

13.2.3 Anonymized data

Anonymized data is not considered as health data under the GDPR and is not protected by professional secrecy. Hence, anonymized data can be utilized more freely. Thus, where use of anonymized data is sufficient, the processing possibilities are wide.

However, anonymization introduce certain challenges. Firstly, the process of anonymization of personal data requires a legal basis and cannot be conducted for any given purpose.[760] With this in mind, innovation, development and research are often considered legitimate interests for anonymization or aggregation of data.

Secondly, anonymization is considered a time-consuming process, which in certain circumstances can be difficult to conduct. The GDPR includes several conditions for data to be considered anonymized. Further, continuous new technology introduces the risk of reidentification of anonymized data. Several cases show that it has proven difficult to anonymize data in a way that allows for researchers, innovators, or others to use the data for the intended purposes. This implies that there are types of data sets which cannot be anonymized or is not suited for anonymization.

Thirdly, through contact with innovation parties in the Nordic health care sector, Deloitte has found that use of anonymized data in innovation project can be challenging as it does not present the possibility of identifying specific data subjects and ask questions that arise over the course of the project. Anonymization also limits the possibilities of identifying patterns, e.g. by combining data sets from different information sources. Thus, due to anonymized data's generalizing character, the opportunities of use can be limited. In these cases, innovators may be forced to

[760] Cf. The GDPR recital 162.

abandon or reinitiate the project, which is both resource intensive and costly.

13.2.4 User generated health data

Generally, health data is collected and recorded by doctors and other health care professionals upon providing health care to a patient, such as through tests and observations in connection with medical examination and treatment. However, health data can also be collected, generated, or gathered outside the health care sector, such as through heart rate monitors, activity trackers, applications, or other similar devices retrieving information regarding users' habits, health etc. User generated health data is generally not subject to professional secrecy and can therefore be utilized to a wider extent.

It is recognized important by market actors in the health sector to enable the use of this type of data, for example to provide patients with better and more personalized health care, as well as to achieve a more patient centered approach. Processing of user generated health data may easily be enabled by the data subject's consent or an agreement with the data subject, cf. this report section 4.3, which may cover subsequent processing for innovation purposes e.g. to improve the product in question. An innovator may also get permission to recontact relevant data subjects to test separate innovative ideas.

Further, the GDPR provides for a right to data portability for processing based on consent or agreement. This gives the data subject the right to receive or transmit its automatically processed data in a structured, commonly used, and readable format. However, the existing Nordic legal framework does not enable individuals to directly transfer user generated data to their medical records. Only health care personnel have the authority to enter information in medical records. Although market actors in the health sector called for such opportunities, to Deloitte's knowledge, Iceland is the only country in the process of providing individuals the opportunity to retrieve and transfer health data from Heilsuvera to a compatible technical solution.

13.2.5 Transfer of health data within the Nordics

Transfer of personal data in Denmark, Finland, Iceland, Norway, Sweden and Åland is regulated by the provisions in the GDPR, which requires free movement of personal data within the EU and EAA. Thus, in general, any innovator, researcher, or enterprise based in another EU member state may access and process health data on the same terms as nationally based individuals or enterprises. Consequently, there is great potential for both transfer of and transborder access to health data for innovation purposes across these countries.

Although transfer of health data within the Nordics generally is possible on the same terms as domestic transfers, certain restrictions can be found on a national level. For example, in Norway, for access to statistics, Statistics Norway has stated that indirectly identifiable personal data cannot be stored outside Norway. Further, health data derived from biological material can only be transferred outside Norway when a Norwegian researcher participate in an international research project. In Denmark, the Danish Health Data Authority are prohibited from disclosing information from the Danish National Prescription Registry to foreign countries. In Sweden, tissue samples in a bio bank cannot be disclosed to recipients in other countries, unless for the purpose of conducting research.[761] In Finland, although there are no rules restricting foreigners from accessing health data, data application or data request to Findata requires a national identification code. Consequently, there are certain practical challenges for foreigners to access health data in Finland. Additional requirements may in some circumstances apply for transfers to Åland.

Although the Faroe Islands and Greenland have not incorporated the GDPR, transfer of health data on the same premises is possible. However, additional requirements may apply. For example, on the Faroe Islands, a notification to the Faroese DPA is generally required, and on Greenland, restrictions apply for transfers to private operators.

13.3 Main obstacles under existing legislation

13.3.1 Lack of innovation specific regulation

The country specific chapters show that, apart from in Finland, there are no innovation and development specific legislation in the Nordic region, which constitutes a clear obstacle for innovation and development activities. Accessors must generally rely on the data subject's consent, or the application of an exception disregarding professional secrecy for the innovation project in question. Normally, the exception applicable, is for scientific research. The challenge in this regard is to determine the area of application.

Due to lack of definitions and delimitations, assistance from independent third parties may be required to provide an overview over existing legislation and scope of provisions. This may increase cost and complexify the time-consuming process. Further, a significant and costly workload must be conducted prior to commencing the intended innovative activity. Also, the uncertainties

[761] The Swedish Act on Bio Banks chapter 4, section 3.

relating to obtaining relevant permission or approvals under the exceptions presents a significant risk for innovators consequently limiting project initiatives.

The challenge of distinguishing scientific research from innovation and development is the most prominent example in this regard. A conceptual distinction between scientific research and innovation is that scientific research aims at creating new knowledge, while innovation is aimed at applying already existing knowledge. Hence, knowledge created through research can be used for innovation purposes. This applies regardless of whether the scientific research is based on anonymized or non-anonymized data. As existing legislation recognizes the use of health data for scientific research purposes, the use of health data for innovation and development purposes are presumably indirectly recognized by existing legislation. Further, as the society is increasingly data driven, knowledge is no longer only created through scientific research.

Health data can originate from multiple sources, such as applications, tracking devices, and similar technology used in daily life. Through powerful processing, such as AI, identification of advanced patterns can further contribute to new knowledge. Such information can substitute traditional hypothesizes and the use of scientific methodology, which under existing legislation are requirements for activities being characterized as scientific research. For these reasons, the distinction between scientific research and innovation and development is gradually further blurred. Thus, due to the technological development, there is an increasing need for specific innovation and development legislation.

13.3.2 Decentralized information structure[762]

The country specific chapters show that the process of accessing health data can be both complicated and time consuming. Across the Nordics, different types of health data are kept in multiple information sources, hereunder medical records, national health registries, national archives, and biobanks, which often are regulated by different legislations, managed by different data controllers or registry keepers, and supervised by different authorities. The specific access procedures vary and are dependent on the type of health data and where it is kept. Although there have been several initiatives to establish centralized processes for access to health data on a national level, there are no national centralized systems in the Nordics. Nor are there any optimized centralized search monitors for identifying where different types of health data are kept. However, at the time of this report, Finland and Denmark have progressed further than the other countries and self governing territories in the Nordic region in this respect.

Due to decentralized information structures and complicated access procedures, there is a risk of valuable health data not being identified nor included in data sets requested for defined purposes of use. Thus, lack of such centralized registries represents a significant obstacle under existing legislation, ultimately hindering development and innovation activities on a national level, as well as transborder cooperation across the Nordics.

As an example, in Denmark, health data is stored in multiple registries managed by different data controllers. The allocation procedure and guidelines for approval for access varies between the different registries, and the application process often consists of several steps. Also, additional permission from relevant authorities is often required. Although the national data catalogue provides details on how to apply for access to health data from the different information resources, and ID-numbering makes it possible to link data from different registers, the application process can be both complicated and time consuming. Due to complex application processes, guidance from third parties may be required, which further complicates the process and enhances the cost. However, as Finland, Denmark has advanced in establishing systems facilitating for access to health data. The national data catalogue provides an overview of most of the available information resources, and guidance on the application procedures for the different registries. The challenge in this regard is that health data is still stored in multiple registries, and that smaller registries are not publicly searchable. Thus, there is a risk of incomplete search results. Further, and more importantly, Denmark has established multiple search machines, which enables access to health data from multiple registries simultaneously. Although these research machines facilitate access to an increased amount of health data, there are no existing search engines including data from all available registries or for other than research purposes. In addition, as health data generally is divided according to the data source rather than its content, it can be challenging to identify and assemble all relevant information for a specific project.

The system of information resources in Greenland and the Faroe Islands are similar to the system in Denmark. However, due to smaller institutions and more limited financial resources for providing data and statistics, the information resources are less advances and comprehensive in comparison. Further, Greenland and the Faroe Islands have not established any national catalogues or research machines.

[762] For more information of similarities and differences between the Nordic information resources, please refer to the report A vision of a Nordic secure digital infrastructure for health data: The Nordic Commons (Nordforsk, 2019).

Amongst the countries and self governing territories in the Nordic region, Finland has advanced the furthest in establishing a fully centralized system for access to health data. Although controlled by different data controllers, Finland has established several information systems enabling centralized electronic archiving. The Finnish Kanta services is an example of such an information system, which enables centralized electronic archiving of medical records and long term storage of data. Further, Finland has established an authority called Findata, which serves as the first point of contact when health data is required from multiple data controllers. Through Findata, Finland has a centralized system for collection and administration of information requests pertaining to multiple controllers of health and social data. Presumably, the establishment of several centralized information systems and an authority administrating access applications and requests to all health data will benefit all interested parties, enhance the process of collecting and obtaining health data, and lowering the administrative burden and cost connected to such access. Thus, the Finnish information structure may serve as an inspiration to the other countries and self governing territories in the Nordic region. At the time of this report, the main challenge related to the newly established Finnish information system, which affect foreign clients especially, is that data requests are only possible to submit with a Finnish personal identity code via the Suomi.fi identification portal. This limits the possibilities for data access for foreign clients. However, Findata is mapping alternative secure identification applications for those not possessing a Finnish personal identity code.

In Greenland, the Faroe Islands, Iceland, Norway, and Sweden, the situation is different. Health data is stored decentralized and managed by several different data controllers. There is no centralized system in place for collection of health data, neither anonymized nor-non-anonymized information. Nor is there a centralized authority that administrates data requests and enables access to data from multiple information sources. The existing structure imposes a risk of data lock in, meaning that valuable data is not captured by a data set for the purpose of e.g. innovation or development. Norway is in the process of centralizing the application procedure for access to health data in different national health registers through the access service Helsedata, which will have a similar authority as Findata has in Finland. In Sweden, there have been several initiatives to facilitate searches for and access to health data. One of these initiatives is the meta data search tool called RUT, established by the Swedish Research Council. RUT enables researchers to obtain an overview of what type of information that is contained in specific health data registries (including quality registries) so that they more precisely can specify their data requests. For access to the tool, an application to the Swedish Research Council is required. Another Swedish initiative is the Region Stockholm's Centre for Health Data (*Swe*: Centrum för hälsodata), aimed at centralizing access to health data through coordination of secrecy assessments and the procedures for disclosing health data. Through this initiative, researchers can submit a disclosure application with the Centre for Health Data only, and not be dependent on the approval from several different agencies. Further, at the time of this report, the University of Iceland is working on developing a search portal similar to the Danish search machines for health data for scientific research purposes called Heilsubrunnur. A weakness of all these initiatives is that they regard specific regions and purposes and does not facilitate a national overview of all available health data.

13.3.3 Additional permit requirements

In addition to approval from each relevant data controller, for access to health data for specific purposes, permits from relevant authorities can be required. Possible additional permit requirements, which apply due to multiple laws regulating access to health data across the Nordics, further complicate the application procedure. Also, it increases the need for assistance and guidance from independent third parties to obtain an overview of the regulations, which increases cost. Due to administrative uncertainty and need for guidance from independent third parties, additional permit requirements pose as an obstacle for access to health data.

Across the Nordics, access to health data first and foremost is dependent on the approval from relevant data controller or controllers. In Denmark, additional permission from relevant authorities are generally required for access to health data for scientific research purposes. Relevant authorities are typically a scientific ethics committee or the Danish Patient Safety Authority and, for projects involving testing of medicines, the Danish Medicines Agency. In addition, a permit from the Danish DPA may be required. The situation is similar in Greenland, the Faroese Islands, Iceland, Norway and Sweden. In Iceland, additional approval from the NBC is required for access to health data for scientific research purposes and, at the same time, the committee grants access to health data for the purpose of the research in question. When applying for research permit and access to health data, a declaration from the relevant data controllers stating that they will provide access to the data must be included. In addition, as the relevant authority, the Icelandic DPA receives a summary of NBC's applications, which describes the processing of personal data that will be carried out in the interest of the research in question. In Norway, additional approval from REC is required for such purposes. Equivalent to the Icelandic process, REC assesses whether access to health data shall be granted, regardless of professional secrecy. At the time of this report, Norway is in the process of establishing a service called Helsedata, providing a centralized point of access to health data from certain data controllers. The service will result in only one necessary approval.

As mentioned above, Finland stands out compared to the other countries and self governing territories in the Nordic region, as no additional approval requirements apply. Findata serves as a single point of access to all health data, meaning that an accessor is unreliant on multiple data controllers or any additional authorities. Thus, in this regard, Finland has advanced further than the other countries and self governing territories in the Nordic region, establishing a clearer regulatory framework and procedure for access to health data facilitating innovation and development activities.

13.3.4 Lack of standardization and interoperability

Another obstacle for accessing health data is connected to standardization and interoperability. Within the health sector, standard deviations, different record solutions, and lack of interoperability occur. The consensus appears to be that there is a need for interoperable data and platforms enabling free and secure flow of health data. Although these challenges are more practical than legal, they limit internal and external communication between different systems, ultimately hindering innovation and development activities across the Nordics.

Although some countries have well established systems for electronically stored health data, the level and quality of such electronic stored health data varies across the Nordic. Limited electronically available health data complicates the process of all health data necessary for specific secondary use purposes, as it can be complicated to identify what information is collected and where it is stored. Further, another issue hindering secondary use of health data is limited standardization requirements. Even when health data is available in electronic form, the quality and content of the health data can vary, making it difficult or impossible to analyze. To achieve adequate exchange of health data, hereunder user generated health data, health data from health databases and registries, and enable use of compiled data sets, it is essential to ensure national standards. Although some of the issues linked to interoperability are solved on a national level, improvements remain to facilitate for seamless access to health data both nationally and across the Nordic.

In Finland, service providers keep health and social data in electronic form, and Finland has a long tradition for developing digital services for the social welfare and health care sector. Thus, Finland has come far in terms of electronically stored health data. As mentioned above, access to electronically stored health data in Finland is limited to citizens with a Finish national ID-number, which hinders access to health data across national borders.

Another country which has come far in this respect is Denmark. The Danish health care sector has high-quality information resources and well-established digitalized register practices, and public and private health care providers are required by law to keep medical records,[763] which are primarily kept electronically. However, a challenge in this respect is that different Danish health regions use different electronic medical record systems, which may limit access to all health data for both primary and secondary purposes.

Iceland has progressed in terms of electronification of health data in general and medical records specifically. However, although it is stated by law that health care facilities shall keep medical records electronically to the extent possible, health care facilities are not required to have interconnected electronic systems for medical records. As use of such systems are voluntary, it is difficult to ensure fully national incomparability. Regarding transborder interoperability, the Icelandic Health Records Act does not limit transfer of health data to national information systems only, nor prohibit transborder linkage of health data. However, challenges in this regard are that Icelandic medical records are not accessible to foreign health care facilities may when treating an Icelandic patient, and that the act only applies to treatment provided in Iceland. Further, although Icelandic law does not require patient consent for transborder access to health data, individuals can restrict access to data to the interconnected system only. At the time of this report, it is not clear whether this right will apply if interconnections are made available transborder or if the data subject's explicit consent will be required.

The Norwegian government has proposed an act on e-health. If adopted, it will be mandatory for relevant actors in the health sector, such as municipalities, county municipalities, health enterprises and businesses, to consider the need for national cooperation and interaction when working with different e-health solutions. This will increase the interoperability within Norwegian e-health solutions.

The Norwegian health sector has also adopted a Code of Conduct for information security and data protection in health care and information security.[764] The aim of the code is to ensure a holistic approach to information security for all organizations within the sector, thus contribute to necessary cooperation and exchange of health data.

In Sweden, there is no legal requirement to keep or store medical records electronically, nor to connect any electronical records to a shared national system. It is however, with the consent of the patient, legally possible

[763] Cf. the Danish Authorization Act chapter 6.

[764] The Norwegian Code of Conduct for information security and data protection in health care and information security version 6 (Norm for informasjonssikkerhet, Normen).

for a health care provider to grant another health care provider electronical access to a patient's medical record by using integrated systems. Information security requirements apply to using such integrated systems, but there are no requirements on standardization nor interoperability. In practice, the medical records are usually shared either by the health care providers using the same system for medical records, or by being interconnected by a technical infrastructure designed for sharing medical records.

13.3.5 Additional country specific obstacles

Iceland: Limited access to medical records of deceased

In Iceland, access to medical records of deceased for innovation purposes is limited for material reasons. Such medical records are transferred to and preserved indefinitely at the NAoI. However, if access is provided to relatives, the relatives may subsequently grant access to third parties for innovation purposes. The Icelandic Data Protection Act applies for processing of personal data of deceased up until five years after the time of death.

Access to medical records of deceased is further complicated as only public health care providers are obligated to transfer health data to the NAoI. For private health care providers, upon resignation of the doctor, vital health data of living individuals are no longer part of the interconnected system. In addition, the level of preservation of medical records and frequency of transfers to the NAoI varies between the health care facilities. At the time of this report, NAoI is yet to receive any electronic medical records.

Sweden: Disclosure reliant on two different assessments

In Sweden, regardless of whether the intended processing of personal data is in accordance with the Swedish data protection legislation, personal data cannot be disclosed from public agencies to external parties without a secrecy assessment.

Secrecy requirements apply unless the information can be disclosed without damage or harm to the individual or any related parties. For health data registries, the requirements are stricter, as disclosure is only accepted either if the information disclosed is to be used for research or statistics, or if the information is restricted from attribution to an individual, e.g. by containing name or any other personal identifiable information. If is further required that the information can be disclosed without damage or harm to the individual or any related parties.

In theory, the secrecy assessment is separate from the disclosure assessment under the Swedish data protection legislation, in which focus of the assessment is on eventual harm a disclosure would cause an individual. However, in practice, whether subsequent processing of the disclosed information is compliant with the Swedish data protection legislation is also of relevance. Thus, the relation between the secrecy assessment under the Public Access to Information and Secrecy Act, and disclosure assessment under the Swedish data protection legislation is complex and not fully clarified.

Regardless of any introduction of innovation and development specific regulation, the strict secrecy regulations could hinder processing of health data for such purposes. For example, for processing of health data from quality registries, a small sized enterprise performing innovative activities can be denied access if there is a risk of harm to an individual.

13.4 Final remarks

The existing Nordic legislation concerning secondary use of health data for innovation and development purposes does not support national strategies and initiatives emphasizing the importance of increased accessibility to health data for the future of health care. To facilitate for data driven health care, access to health data for other purposes than treatment and scientific research is necessary. Although processing of health data for innovation and development purposes may be covered by existing legal bases, the area of application is unclear. Further, several innovation activities will never be covered by existing legal bases and are reliant on the data subjects' consent. The GDPR allows both processing of health data for reasons of significant public interest, as well as for several health related purposes. Corresponding provisions are laid down in Faroese and Greenlandic legislation. Consequently, there are legal possibilities to establish a framework facilitating the utilization of Nordic health data.

Processing of health data for innovation and development require an additional national legal basis. This legal basis must be proportionate to the aim pursued and contain appropriate safeguards ensuring the data subjects' fundamental rights and freedoms. Such measures may include limitations on the type of data subject to processing, requirements on data format, or processing environment, e.g. data sandboxes. Other possible measures include data minimization, limitation of storage periods, encryption, pseudonymization, access control, requirements on local rather than central processing, or requirements on distributed algorithms and distributed learning.[765]

[765] Kunstig intelligens og norske helsedata, Teknologirådet (2019).

As it is challenging to secure the data subject's fundamental rights and freedoms when increasing accessibility to health data, future legislation on secondary use of health data should focus on how to regulate and legally formulate such measures, rather than merely focusing on lawful purposes.

14. Appendices to the report

14.1 Appendix 1 - Members of Reference Group

- Bogi Eliasen, Associated Partner, Copenhagen Institute for Future Studies
- Anne-Katrine Nielsen, Senior Development Manager, Copenhagen Health Tech Cluster
- Kathrine Myhre, CEO, Norway Health Tech
- Anders Tunold-Hanssen, Managing Director, Nordic Interoperability Project AS
- Kristinn Gylfason, Compliance Officer, Sidekick health
- Ingi Steinar Ingason, Team Leader for National Center for eHealth at Directorate of Health in Iceland

14.2 Appendix 2: Relevant definitions from the GDPR

Article 4 (1) '**personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Article 4 (15) **data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Article 4 (2) "**processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Article 4 (7) "**controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Where two or more controllers jointly determine the purposes and means of processing, they shall be **"joint controllers"** cf. article 26.

Article 4 (6) '**filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Article 4 (11) **consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Article 4 (5) '**pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Article 4 (13) '**genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Article 4 (14) **'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Article 4 (21) **'supervisory authority'** means an independent public authority which is established by a Member State pursuant to Article 51;

This publication is made as part of Nordic Innovation's **Health, Demography and Quality of Life** program to support the vision of making the Nordic region the most sustainable and integrated health region in the world by 2030.

Nordic Innovation

Stensberggata 27
NO-0170 Oslo
Norway
www.nordicinnovation.org