Digital Health Revolution

PERSON CENTRIC DATA MANAGEMENT MODELS AND OPPORTUNITIES IN THE HEALTHCARE SECTOR

THE NORDIC WAY
This document was produced by:
Copenhagen Institute for Futures Studies
Amaliegade 5C
1256 København K
Denmark

Centre for Health and Technology
Faculty of Medicine, University of Oulu
Aapistie 5
FI-90014 University of Oulu
Finland

Contact Person:
Bogi Eliasen, Associated Partner
be@iff.dk / +45 6082 6226

Authors:
Bogi Eliasen
Kevin Tan
Laura Prisca Ohler
Emilie Lindeburg
Maritta Perälä-Heape

Supported by:
Digital Health Revolution Project, funded by Tekes – the Finnish Funding Agency for Technology and Innovation

May 2018
Foreword

For many years, the European Union has recognised the need to harmonise data privacy laws across the region, and to impose stronger protections for its citizens. Today data is increasingly being generated, stored and used by various public and private bodies. In 1995, when the previous Data Protection Directive 95/46/EC took effect, only an estimated 1% of Europeans were on the internet in 1995. Since then we have seen the introduction of social media, widespread personal mobile devices and cloud storage, as well as new methods of covert data collection. Therefore, there is a need to update European data privacy laws to keep pace with technological progress.

General Data Protection Regulation (GDPR)

Beginning 25 May 2018, the new European General Data Protection Regulation (GDPR) will be enforced. This has followed several years of discussion about how new protections should be updated to reflect the emerging digital landscape of data processing and data controlling. The GDPR regulations replace the older Data Protection Directive 95/46/EC from 1995. The new GDPR will enforce sweeping changes, including:

- **Increased territorial scope**: new regulations will now apply to all companies that process the personal data of subjects residing in the EU, irrespective of the company’s location (ie. non-EU based companies)
- **Hefty penalties**: Increased fines of up to 4% of annual global turnover, or 20 million (whichever is greater), in the event of non-compliance.
- **Consent**: Long, illegible terms and conditions full of legal jargon will no longer be an acceptable form of consent. Withdrawal of consent must also be easy to execute.

Other key changes will revolve around new Data Subject rights, recognising the view of data privacy as essentially a human right. These include:

- Right to breach notification
- Right to access one’s own data - in particular, to be able to access it free of charge and within a reasonable time frame (ie. one month)
- Right to have one’s data be forgotten
- Right to data portability
- Right to privacy by design
- Right to access Data Protection Officers

In particular, this paper will focus on the right to privacy by design, referring to potential future data management models where data subject rights are designed into the framework, rather than additions as mere afterthoughts.

A New Digital Reality

The accelerating pace of technological development is changing many aspects of both the society and how we live as individuals. We are entering the 4th Industrial Revolution with the combination of data, biology and materials that greatly impacts many domains of health. Data is produced in an increasing number of settings and the ability to use data for knowledge, services and treatments expands every day.

Over the past 150 years, the journey of health and medicine has told a tale of pioneering discoveries and extraordinary success. The advent of antibiotics brought about a paradigm shift as it broadened new scope for aggressive therapies. Limits were pushed, then shattered as medical specialisation scaled up to population level care. Identical treatments worked well for patients with identical diseases. Epidemiology and randomised control trials have no doubt saved millions of lives.

In 1953, DNA was discovered and many years later, the first human genome was fully sequenced. This shed further light on the origins of disease. The ability to characterise cells on a molecular level held promise of a new type of targeted therapy, unique to each individual, and signalled the end of ‘the average patient’. A new paradigm of personalisation was born. In 2015 former US President Barack Obama called precision medicine “one of the greatest opportunities for new medical breakthroughs”. In this new approach, improvements in health and treatments would be derived from personalized care, tailored to an individual’s genes, environment and lifestyle.

---

1 https://www.eugdpr.org
These are remarkable visions for the future, but how do we get from our current, often fragmented, state of healthcare to this new, improved era? And as healthcare becomes increasingly digitalised, all aspects of data including storage, security, privacy and operability will come under greater scrutiny. Governments will face increasing pressure to fulfil the promises of precision medicine while protecting citizen rights. This task can only be achieved with a more cohesive and transparent data infrastructure and protections that balance privacy with innovation. Furthermore, in our increasingly globalised societies, data interoperability between nations will be crucial to capitalise on population insights as we tackle some of the most pressing public health issues of our times.

The digital health revolution is here, and it places health communities at a crossroads. The choices we make today about how our healthcare data is managed, controlled and utilised will shape the future terms of reference. This paper sets out the current landscape of digital healthcare data management, particularly in the European context, and explores a new way of transacting healthcare data so that our common objectives of transparency, value and individual empowerment can be achieved.

As we search for new personal healthcare data management models, perhaps there is no better place to start than in the Nordic region. Famous for their extensive population registries, Nordic countries possess a wealth of quality data on its citizens. With digital literacy high in the Nordics, access to some of this healthcare data is managed through Health Information Portals. Finally, social trust, including trust in public healthcare institutions, is also uniquely high within the region^4, a necessary ingredient for public engagement during uncertain times of digital transitions. These conditions create the perfect opportunity for the Nordic region to be a world leader in defining future data management models that ensure people, and patients, remain at the core.

A crucial part of the development is the ability to set data free and work with data in new portable and interoperable settings. This is a fundamental aim of the MyData movement – to empower people with data rights, control and access to their own data, while simultaneously fostering innovation and value for citizens. An example of this application would be in the field of personalized health.

This paper will discuss some of the exciting work forging ahead in the Nordic region. The Digital Health Revolution (DHR) project, launched in Finland in 2014, proposes a person centric data management model that empowers individuals to control the use, exchange and management of their personal health data^5. The foundations of DHR is built on principles of MyData, which are:

1. Human centric control and privacy
2. Usable data
3. Open business environment

The details of the DHR project and MyData ecosystem, as well as a possible Nordic model of healthcare data management, will be discussed at depth. This white paper was produced as part of the Digital Health Revolution project funded by Tekes, the Finnish Funding Agency for Technology and Innovation. The development of the paper benefited significantly from generous input and support provided by our outstanding sponsor and reviewers, reflecting a balance of corporate, NGO, government and academic institutions. The study was conducted with the close collaboration with the University of Oulu, which has been initiating and leading the DHR project. While MyData is not the only way to work with the emerging opportunities and challenges of health data, it does set a cohesive frame and is possibly the most development frame to work with person centric data management.

Global Megatrends
The pressure for a digital health agenda can also be considered in the context of global megatrends. This term refers to synthetic, complex aggregations of trends that exert a forceful impact on businesses, societies, economies, cultures and personal lives. The Copenhagen Institute for Futures Studies works with fourteen megatrends shown in the diagram on the right.

---
^4 Andreasson U. Trust - the Nordic Gold. Denmark: Nordic Council of Ministers, 2017
^5 http://www.digitalhealthrevolution.fi/research-themes.html
Demographic development, technological development, knowledge society and individualization are some of the strongest megatrends behind the digital health agenda. Commercialization, acceleration and polarization are also important considerations when planning the future health data infrastructure and management models in the Nordic setting. Naturally, these megatrends will also interact with the local environment and reflect the socio-political context.

On a societal level, the growing P4 movement in healthcare recognises predictive, preventive, personalised and participatory medicine as a sustainable vision of the future. Not only does this mirror a mindset change of health as a proactive and not reactive responsibility. It also reflects an overwhelming convergence of three global phenomena that are sweeping across the field. They are, the recognition of systems biology to decipher disease complexity, the increasing role of digitalisation in healthcare, and the rise in consumer access to information and participation in their own management. Meanwhile, the introduction of new GDPR regulations demonstrates the political context in which data rights will evolve.

Revolutions are fundamentally about change, and Europe is arguably undergoing one of the largest transitions in modern history. As with any transition, the beginning poses difficult questions, the middle is fraught with challenging work, but by the end we cannot imagine how things used to be. Visions of a global digital future in healthcare will inspire some, while leaving others feeling deeply uncomfortable. Both responses are valid and should be welcomed, for alongside the digital aspects of change we will need equal transformation in the cultural sphere, ignited through public debate. There will, of course, be uncertainty in the coming years around the control and uses of healthcare data. And while nobody can predict the future with absolute certainty, there is one thing we can be sure of - to do nothing is no longer an option. Our data is out there and it is being used.

---


7 https://www.eugdpr.org/
Overview of the White Paper

This paper aims to clarify the current state of healthcare data management, and what central challenges and opportunities lie ahead for person centric health data management in the Nordic region. It will also provide recommendations and a roadmap to realise this health data ecosystem.

The report is structured as such:

- **Section 1 – Your Digital Self**
  - Personal Data – the different types, and how they can relate to health data
  - Behavioural Data
  - Data in the 21st century
  - The Nordic region – Healthcare data from population registries
  - Nordic health information portals – the current state

- **Section 2 – New European Data Regulations**
  - GDPR in the context of healthcare data
  - Consent in the new GDPR
  - Navigating through GDPR

- **Section 3 – Introducing Person Centric Health Data Management**
  - Introduction to the Digital Health Revolution (DHR) project
  - MyData principles
  - Why is MyData needed and its benefits
  - Digital Health Revolution project in more detail

- **Section 4 – Cases**
  - Australia – My Health Record
  - United Kingdom – DigiMe
  - Switzerland – Med’Profile
  - Sweden – Hälsa för mig
  - Finland – My Kanta pages

- **Section 5 – Opportunities**
  - A model case – My Nordic Health Record Card (NHRC)
  - Patient benefits
  - Societal benefits
  - Business benefits

- **Section 6 – Ethical challenges of a MyData ecosystem**
  - Selling vs Sharing Data
  - The Me in We
  - Winners vs Losers
  - Anonymity vs Precision
  - Nudging vs Coercion
  - Precision Medicine vs Precision Health

- **Section 7 – Future Game Changers**
  - Blockchain technology
  - Big Data in the era of Artificial Intelligence
  - Big Data, Big Error?
  - Value-based healthcare
  - International Health Account Number (IHAN)

- **Section 8 – Recommendations and Roadmap**
## Definitions

<table>
<thead>
<tr>
<th>Word</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface (API) enables to connect different devices and applications, which allows users to place an order, make reservations, book flights etc. APIs make it possible for different programmes to “talk” to each other. An API is the messenger that takes requests and tells a system what you want to do and then returns the response back to you.⁸</td>
</tr>
<tr>
<td>Creative Commons</td>
<td>Creative Commons is a provider of copyright licenses. The company helps to legally share knowledge and intellectual property between users.⁹</td>
</tr>
<tr>
<td>GDPR</td>
<td>The General Data Protection Regulation (GDPR) will come into force in the European Union (EU) in May 2018 to meet current challenges related to personal data protection and to harmonise data protection across the EU. The GDPR is anticipated to benefit companies by offering consistency in data protection activities and liabilities across the EU countries and by enabling more integrated EU-wide data protection policies.¹⁰</td>
</tr>
<tr>
<td>Health information portal</td>
<td>The Health information portal is a web-based access point that enables self-serve health IT services for patients. Patients can view all their health information (reports from doctor visits, results of lab tests, immunization records, payment processing etc.) inserted by healthcare professionals. Users can schedule appointments, order prescription refills, download forms, and communicate with their doctors via mail.¹¹</td>
</tr>
<tr>
<td>Person-centric models</td>
<td>The individual is in control of her/his own data management and decides what and with whom their data can be shared.</td>
</tr>
<tr>
<td>ICT</td>
<td>The information and communications technology (ICT) is the infrastructure and components that enable modern computing. ICT cover all devices, networking components, applications and systems that combined allow people and organisations to interact digitally.¹²</td>
</tr>
<tr>
<td>QALY</td>
<td>A quality-adjusted life year (QALY) is a unit often used in cost-benefit analysis, which predicts both the quality and duration of life after medical or surgical treatment.¹³</td>
</tr>
<tr>
<td>Systemic-centric or centralised models</td>
<td>The government, organisations, NGOs, or corporations are in control of a person’s data and their decisions. The individual has no or limited control of his/her own data.</td>
</tr>
</tbody>
</table>

Table 1: Definition of key terms used in this paper.

⁸ https://www.e-conomic.dk/regnskabsprogram/ordbog/api
⁹ https://creativecommons.org/about/
¹¹ http://whatis.techtarget.com/definition/patient-portal
¹² http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies
¹³ https://en.oxforddictionaries.com/definition/qaly
Section 1 - Your Digital Self

Personal data
As technology integrates deeper into our personal and professional lives, the more digital data is being generated, collected and utilised. As data complexity grows, there is an increasing need for a common understanding of what personal data means. According to the EU GDPR regulation, personal data refers to ‘any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. Evidently, the definition is very broad, enough to encompass the many domains in our lives that data has now encroached upon.

Health and Medical Data
Many of us are familiar with our health data being collected through formalised channels. For example, clinical data on a person’s medical diagnosis, blood type, prescriptions and allergies are stored by GPs and hospitals, while anonymous population data may be collected through public health registries. As hospitals worldwide undergo transformation towards electronic health records (EHR), data portability and interoperability can be a challenge for incongruent platforms. Nevertheless, this type of health data is normally strictly regulated, requiring the citizen to provide informed consent at the point of collection. In most Nordic countries the aggregated, anonymized health data is stored in national or regional population registries, to be used for quality and administrative purposes. Furthermore, citizens and health professionals can view and access some of their health data through national Health Information Portals, but this is not currently interoperable between the Nordic countries. Table 2 and Figure 2 provide more details on country-specific Health Information Portals and population health registries.

Behavioural Data
In more recent years, the amount of behavioural data collected on individuals has grown enormously. Personal devices such as mobile phones, computers, wearables, customer loyalty cards and social media have facilitated a new form of personal data collection. The data collected from these personal devices converges to form a digital self, who leaves a digital footprint with enormous behavioural insights about the user. Some of this is behavioural data may be considered health-relevant, for example what food you eat, whether you smoke, how often you smoke, how far you walk per day, your resting heart rate and sleep-wake cycle. Other types of behavioural data may be more relevant for social and financial sectors, such as impulsivity, shopping habits or preferred social networks, which may be inferred from who you call, text and email most frequently.

---

14 https://www.eugdpr.org/gdpr-faqs.html
Behavioural data is fast becoming the new game changer in the digital healthcare landscape. The internet of things (IoT) has allowed us to embed sensors into everyday objects, generating real-time data feedback. Furthermore, as these household and wearable objects become smarter, they start to eliminate the need for human input during data collection, thereby minimising sources of input error, manipulation and improves consistency of data hygiene. There are yet other types of behavioural data intersecting with health, such as digital behavioural change interventions. These services may be offered through mobile coaching apps, SMS and custom websites. As governments struggle to keep pace with the accelerating expansion of technology, industries have stepped into market with little or unclear regulation.

**Data in the 21st century**

The saying “greater than the sum of its parts” has never been truer of data, and it is one of the reasons data holds such value. As the amount of data accumulates and analytic and statistical capabilities improve, behavioural data shifts from being mere surrogate reflections of our behaviours, to active insights about our identity, motivators and preferences. Many believe that such targeted and distinctly personal information has the ability to influence our future behaviours. It is no wonder that in 2016, The Economist declared data, and not oil, as the world’s most valuable resource of the 21st century.

Given the value of this commodity, several questions naturally arise:
- What data already exists about me?
- Where is this data stored?
- How is it protected?
- How is this data being used?
- When can I access my own data?
- Who owns my data? (And why is it not me?)

That most of us cannot comfortably answer these questions raises red flags about the current state of personal data management. In the healthcare sector, this demands even greater concern due to its intimate and confidential nature. The absence of public policy to specifically address these concerns has done little to assuage public scepticism. Meanwhile, the total volume of personal health data continues to grow each day, and along with it, the pressure for a new model of transparent health data management.

Some public concerns have been raised about the uses health data that are already taking place today. Some examples include:
- Insurance premiums being scaled based on customer willingness to be monitored by personal monitoring devices.
- Workplace monitoring as a result of access to healthcare data.
- Collaboration between Google-owned AI company DeepMind with the Royal Free NHS Trust, which gave access to healthcare data on 1.6 million patients across three London hospitals. Some of this included sensitive information such as abortions and HIV status.

Ethical questions of privacy and ownership are not the only concerns. There is also the issue of duty to deliver. If societies are to invest in and consent to collecting all this healthcare data, how do we extract its value for the benefit of both the individual and for the population’s health? Using precision medicine as an example, if we are to draw meaningful conclusions from genomic data and their effect on predicting disease and treatment response, there will need to be more user-friendly and interoperable forms of data sharing. Data from different sources such as municipalities, regions, states, even between nations and from private organisations could be useful to conduct population-wide studies. Yet in the current state of data management, citizens may question the benefit of sharing their personal health data. Finally, there is the very practical challenge of data interoperability. To put it simply, ‘not all data

---

speaks the same language’. As we will see in the next section, not even the Nordic countries with their long tradition of population registries, currently share common data operability. The need for a new model of patient data management is clear, particularly one that places citizens at the helm of their own data. However, this paper will first discuss existing health data registries and Health Information Portals in the Nordic Region.

**Nordic Registries – theoretical goldmine, barriers in practice**

In the Nordic countries, a person’s individual health record is collected from birth. While the registries and portal interface vary depending on country, these formal channels of health data collection are operated by public-run health organisations, for the purposes of quality control, research and to alert of public health threats.23

Figure 2 summarises the current status of national and regional health quality registries in the Nordic countries. Although the comprehensive registries make it theoretically possible to combine data to form a larger Nordic cohort, there are many practical challenges in doing so.24 Coding systems differ between countries, and some are omitted. Experience in retrieving data is variable, as are the laws that govern permissions to save key codes, which allows future retrieval of linked data for longitudinal information. Different levels of ethical clearance are mandated by each nation, and finally the data sets need to be aligned into the standard format to be interoperable. Such obstacles make it very hard to establish Nordic collaborations in practice today.24

**How do Nordic citizens access their medical and health data?**

In Nordic countries, an individual can access their own health data through a Health Information Portal, for information such as medical diagnosis, drug prescriptions, allergies etc. Table 1 provides a brief comparative analysis of the Health Information Portals in each Nordic country. Similar to the registries, each country has its own portal and these are not interoperable between Nordic nations. Furthermore, while some countries are investigating incorporating health-related behavioural data (e.g. from personal wearables) into national portals, this very much remains in the infancy stages. As each Nordic country upgrades its own population registries and Health Information Portal, political changes in the EU data protection space are taking place.

---

Appendix Figure A: Overview of population health and quality registries in the Nordic countries today

SWEDEN

108 national quality registries

Categories include: Cancer, circulatory system, dental care, elderly palliative care, emergency anaesthesia and intensive care, endocrine organs, eyes, infection, lung diseases, musculoskeletal system, nervous system, other areas, paediatric obstetrics and gynaecology, psychiatry and stomach and intestines

DENMARK

75 regional and national health quality registries

The registries broadly cover: cancer, non-neoplastic elective surgery, cardiovascular diseases, emergency care, psychiatry, obstetrics and miscellaneous.

FINLAND

An estimated 60+ national and regional quality registries

It should be noted that some of the regional registries are in the planning phase. The precise number and names of the registries are not all publically available to search.

ICELAND

2 main types of registries

Some belong to the Directorate of Health, others to the Landspitali (biggest hospital in Iceland).

DOH: 11 registries (some maintained by patient associations)

Landspitali: 14 registries

NORWAY

54 national health quality registries

Categories include: Cardiovascular diseases, cancer, diabetes, gynaecology, rehabilitation, infections, psychiatry, paediatrics, auto-immune diseases, nervous system, stomach and intestines.

REFERENCES

a, c, d, e: https://www.nordforsk.org/no/programmer-og-prosjekter/prosjekter/guide-for-international-research-on-patient-quality-registries-in-the-nordic-countries;
b, http://www.rkkp.dk/om-rkkp/de-kliniske-kvalitetsdatabaser/
<table>
<thead>
<tr>
<th>Sweden</th>
<th>Denmark</th>
<th>Norway</th>
<th>Finland</th>
<th>Iceland</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>1177 and Läkemedelskollen</td>
<td>Sundhed.dk and Medicinkortet</td>
<td>Helseenor</td>
<td>Kanta</td>
</tr>
<tr>
<td><strong>Responsible institutions</strong></td>
<td>1177 owned by 20 Swedish Regions, Läkemedelskollen by eHealth Authority</td>
<td>Danish Health Data Authority</td>
<td>Directory of eHealth</td>
<td>Kola, THL, Ministry of Social Affairs and Health and others</td>
</tr>
<tr>
<td><strong>Structure</strong></td>
<td>State, regions</td>
<td>State, regions, municipalities</td>
<td>State</td>
<td>State</td>
</tr>
<tr>
<td><strong>Content/scope</strong></td>
<td>1177 information, inspiration and e-services for health and healthcare. Access via web to own health data. Scope differs between the regions.</td>
<td>Sundhed.dk: Contains record and the context in which it has been viewed by professionals, treatment plans, validated health information, database of practitioners, information on health offers in region/municipality. Medicinkortet: Information on prescriptions, contact to GP for renewal.</td>
<td>Citizens can view and add certain information to their journals as well as see in which context their records have been accessed by professionals. Helseenor also allows for change of GP, information on prescriptions and renewal. The portal also contains validated health information on various topics, e.g. lifestyle. Parents can view information on their children until they reach the age of 16.</td>
<td>Kanta includes Patient Data Repository, Electronic prescriptions, My Kanta pages, Pharmaceutical database. Users can see in which context their information has been viewed. Parents can act on behalf of their children until age 10; afterwards they can only view information added before the child reached the age of 10.</td>
</tr>
<tr>
<td><strong>Individual permissions</strong></td>
<td>Läkemedelskollen: Information on prescriptions, purchased drugs, high-cost protection, personal drug records kept in registries</td>
<td>Sundhed.dk: Each person can hide personal health info which will then be marked as hidden information for health staff. If a citizen wants to add information to their record, they must send the information to a physician applying for the information to be added. Medicinkortet: Parents can view information on their children until the age of 15 if born after 2004.</td>
<td>Citizens can control the access to and sharing of their health information in the context of patient treatment and research. Children age 12-16 can choose to hide specific information on their prescriptions from parents in agreement with their doctors.</td>
<td>Citizens examine their own health records via internet and choose what info is shared with health professionals. It is possible to request further details regarding the context in which personal health information has been viewed by professionals.</td>
</tr>
<tr>
<td><strong>Collaboration externally (behavioral data)</strong></td>
<td>Inera, that is owned by the municipalities and regions</td>
<td>Sundhed.dk plans to expand the amount of data linked to each person and addresses data from fitness, medical and support apps (2016-18)</td>
<td>Unknown/unavailable</td>
<td>Covers both public health sector and most of private sector</td>
</tr>
<tr>
<td><strong>Data security</strong></td>
<td>Information is secured with the Swedish encrypted e-ID</td>
<td>Personal access only, except for parents (see above). Authorization can be given to others. In case of an emergency, all hidden information accessible by a health professional. Information is secured with the Danish encrypted ‘NemID’.</td>
<td>Personal access only, however, authorizations can be given to others. Access on behalf of others can vary depending on the authorization given. Information is secured with the Norwegian encrypted e-IDs, e.g. Bank ID.</td>
<td>Personal access only, (except for parents, see above) however, authorizations can be given to others. Data is secured with the Finnish encrypted e-ID.</td>
</tr>
<tr>
<td><strong>Future plans</strong></td>
<td>EHalsa, a new citizen centric platform that also includes self monitoring, reporting and behavioral data. Temporarily halted pending legislative process</td>
<td>Integration of more data sources (including patient generated data)</td>
<td>Currently, not all regions have access to all features. Will be expanded.</td>
<td>Dental healthcare being added, social services data, potential export of portal</td>
</tr>
</tbody>
</table>

Appendix Table A: Comparative overview of health information portals used by Nordic citizens in respective countries today
a. https://www.1177.se
b. https://www.sundhed.dk
c. https://helseenor
b. https://www.landlaeknir.is/english/
Section 2. New European Data Regulation to take effect

GPDR in the context of healthcare data

In the upcoming GDPR document, healthcare data is afforded a special status\(^\text{25}\). It defines data concerning health as “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”. Meanwhile, genetic data is defined as “personal data relating to 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”. Finally, biometric data is defined as “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”.

Personal data that falls under these three categories of health will demand more stringent protections. In particular, processing of these types of data will be prohibited unless one of the following three conditions is satisfied:

1. **Explicit consent** is given
2. **Processing is necessary** for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
3. **Processing is necessary** for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices

What is consent?

Under the new GDPR, consent has been defined in Article 4, Nr. 11 as “any freely given, specific, informed and unambiguous indication of 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”\(^\text{26}\). What then, is explicit consent? This aspect remains unclear, particularly as to how explicit consent differs from 'non-explicit' consent. Will opt-out be considered sufficient to fulfil the definition of explicit consent, or will patients and citizens need to sign a declaratory statement to opt in? These questions, along with other data subject rights will need to be considered in detail in the coming months.

Navigating through GDPR

The changes arising from GDPR will introduce fairer data protections and rights for EU citizens. However, several practical challenges lie ahead with regards to institutional compliance. Organisations that process and control EU citizen data, not least in health, will require clear guidelines to adapt their existing resources or develop new technological solutions. Policies and procedures on data collection, retention and destruction will need to be reviewed and updated, while frontline staff will need to be briefed and trained with the necessary digital literacy and skills. Finally auditing processes to ensure compliance will be required to avoid breaches and hefty penalties\(^\text{28}\).


\(^{26}\) https://gdpr-info.eu/art-4-gdpr/.

Section 3. Introducing Person Centric Health Data Management

In the wake of profound data regulatory changes in the EU, important strategic questions arise. How will the Nordic countries respond to ensure that their health data management models comply with the new regulations? More importantly, is mere compliance sufficient or is there a better model to data management that empowers citizens to be the drivers of their own health data? When the GDPR refers to data privacy by design in line with the EU regulation, perhaps there is a smarter way to design the digital infrastructure and ecosystem so that privacy, but also value, are at the core of all transactions. These questions will be explored in the subsequent sections of the white paper.

Digital Health Revolution Project

As healthcare systems become increasingly digitalised and transition from reactive towards more proactive models of care, new opportunities arise to establish a person centric approach to health data management. With these goals in sight, the Digital Health Revolution (DHR) project was born in 2014. To date, the multidisciplinary research has laid groundwork for the formation of a MyData-based service ecosystem. In particular, it has focused on the technological, regulatory and ethical requirements, as well as service transformation and business model opportunities to implement such a revolutionary ecosystem in the healthcare setting. To this end, the DHR project has released a MyData Service Development Kit to assist software developers in constructing standard, interoperable technological solutions that meet the EU privacy juridical requirements. But first, what is MyData and why is it important?

What is MyData?

Fundamentally, MyData refers to a new approach to personal data management and processing. It is a response to the current, increasingly fragmented state of personal data management, one which lacks transparency and interoperability. With MyData, it shifts the control and access of personal data from organisations to the individual. As previously discussed, personal data can span multiple life domains including retail, communication and media, health, energy, public services and finance sectors. The scope of MyData encompasses all types of personal data, however, the Digital Health Revolution project and the focus of this paper will be on health data.

The three guiding principles of MyData are:

1. **Human centric control and privacy**: individuals are empowered actors, not passive targets, in the management of their personal lives both online and offline - they have the right and practical means to manage their data and privacy.
2. **Usable data**: It is essential that personal data is technically easy to access and use - it is accessible in machine readable formats via secure, standardised APIs (Application Programming Interfaces).
3. **Open business environment**: Shared MyData infrastructure enables decentralized management of personal data, improves interoperability, makes it easier for companies to comply with tightening data protection regulations, and allows individuals to change service providers without proprietary data lock-ins.

---


In light of GDPR, a MyData-based ecosystem of health data management can be considered complementary, and not mutually exclusive to GDPR. This person centric approach to data inherently structures consent in the flow of data. By design, it addresses the right to data portability, right to access and right to have data forgotten. Furthermore, by virtue of infrastructure revamp, MyData ensures the right to privacy by design. Data privacy protection sits at the core of this design, not as a tag on feature.

Why is a MyData approach needed?
As discussed in Section 1, personal data is already being generated, stored and utilised by various sources. In the current climate of data policy, key data aggregators have emerged. Some aggregators are sector specific, such as Validic and Human API in the health field\textsuperscript{30}. Meanwhile, other companies have developed into powerful data aggregators. These include famous household names such Google, Facebook, Apple and Microsoft. Moreover, as new business strategies emerge the distinctions between sector specific aggregators are increasingly blurred. These companies have provided numerous societal benefits, for example, the convenience and speed at which health literature is accessed and retrieved today. This has no doubt democratised health knowledge to many where previously it was unattainable.

However, in the context of health data, several disadvantages arise from this model of personal data management\textsuperscript{30}. First, there is no incentive for data operability (and therefore portability) since users cannot simply take their data to a competing service provider. As a consequence, this type of data hoarding suppresses innovation and research insights, unless they align with the company’s strategic interests. Another drawback is that privacy and transparency become a secondary concern. Since some citizens would withhold consent if they were aware of the extent to which their data was being used, it is more advantageous for these aggregators to retain existing, ambiguous privacy clauses. This erodes public trust, which is further undermined by famous scandals of privacy breaches that circulate the media\textsuperscript{31}.

Benefits of a MyData-based infrastructure
A person centric approach to data management, alongside new GDPR regulations, would allow willing individuals to consent to their data being utilised, either for social or commercial purposes. This would happen in a more open and transparent way. This fosters trust, reduces the likelihood of companies breaching GDPR or similar data protection regulations, while increasing the value of data through interoperability and open aggregation.

Exemplified here is how individual profile data, consumption data, and activity tracking data could be shared with healthcare services\textsuperscript{32}. The MyData infrastructure can provide standardized methods for managing data logistics between different professional and public health organisations and sources of behavioural data in robust ways across organisations and health care providers. MyData can be applied in various ways of healthcare data management in a human centric way, e.g. by developing new kinds of mobility services, by supporting users with their personal finances, by informing users about their consumption decisions, and by creating new types of research databases.


\textsuperscript{32} Poikola A, Kuikkaniemi, K, Honko, H. MyData - A Nordic Model for human-centered personal data management and processing. Finland: Finnish Ministry of Transport and Communications
Digital Health Revolution Project in detail
How would MyData principles be implemented in a healthcare context? Over the last four years, the DHR project based in Finland has gone about addressing this question. For instance, what unique qualities about the healthcare sector require specific considerations? And how would such a service ecosystem be rolled out in the Nordic region?

The following three research themes of the DHR project have been identified:

**Making value of personal analytics**
This includes studying the value of personal data for consumers and how consumers' data can better open up new practices for personal services. Furthermore, the project is concerned with how new business models can be integrated and developed within MyData-based ecosystems.

**Liberating personal data**
This includes research and prototype development on how to integrate and exchange personal data from various sources, including genomic data, medical history data, behavioral data, as well as consumer, demographic and mobile phone data.

**Connecting data to services**
Central to the project is increasing the end-user perspective in connected health service design. This includes studying people's preferences and usable design solutions for contextual personalized connected health services, as well as the end-user motivation to collect, share and use their personal health data.

Figure 4: Principles of the Digital Health Revolution project

DHR Pilot Study

The Digital Health Revolution (DHR) pilot study was geared towards developing next-generation personalized health intervention. It aimed to integrate longitudinal deep multi-omics profiling, digital monitoring and personal data to reshape healthcare systems with a more holistic, P4 systems biology approach. It achieved this by addressing five critical questions.

The first was how to collect, analyse and integrate comprehensive digital health and wellness data. Over a 16-month period, just over 100 volunteers provided regular samples ranging from laboratory indices, genomics, saliva samples and fitness tests, with a planned follow up for five years. The second question was to assess if personal health and wellness data, coaching, and gadgets and apps help to motivate lifestyle changes. Therefore, the study incorporated health-related data such as physical activity and purchasing behaviour,

paired with personalised health advice and wellness coaching. This was necessary to address the third question, which was how to return this data to people in an actionable format. Finally, the study was designed to assess the longitudinal impact of the lifestyle changes, as well as the normal variation in the molecular profile of a normal adult population.

To date, the DHR project has developed a series of concrete outcomes. A MyData infrastructure has been developed based on Creative Commons licenses, to liberate the potential of personal data and to facilitate its flow from multiple data sources to applications and services via a standard and interoperable consent management framework. The architecture has been defined against the MyData principles to meet and surpass the new privacy related juridical requirements that will be enforced EU-wide, also to ensure standardisation and interoperability. The infrastructure is currently undergoing testing in several pilot studies. However, many challenges remain to be overcome or even fully articulated.

**Lessons learnt from the DHR project:** It became obvious that the usage of data in the person centric service and business development is more complex than was anticipated. Data is not always available, nor in a usable format, thus hindering the integration of data from various sources. Today, data is collected in the registries and information predominantly serves organizations and not people, who are using the digital services and who need more personalized services and digitally aided consultations. Furthermore, the holistic, integrative analysis of data is very costly, while requiring specific expertise in data analytics.

An open business environment for data sharing is only now starting to emerge; a major challenge lies with the identification and application of the most suitable technological solution amongst the many solutions, all of which remain under development. There is a need to develop totally new business models for personal data access and movement between various services. New models for sharing data between individuals, data collectors and third parties are also needed to meet EU-wide privacy regulation related requirements.

The human-centered approach in data management has become a relevant topic when developing person-centric data-led care. The MyData principles (usable data, human centric control and privacy, open business environment) are difficult to fulfill, if major changes at the systemic level do not take place. Furthermore, citizen generated data must be integrated more efficiently during the development of digital services.

Importantly, new roles addressing customer needs require more attention, since the transformation to MyData-based services in healthcare can enable empowerment of the customers. Empowerment will happen only if we understand the expectations and individual capabilities to control and interpret their own data, and ethical concerns related to data sharing. In particular, citizens’ access and management of data relevant to their health and wellbeing is challenging, since data is stored in several public and private repositories and registries with different security mechanisms and consent management structures. There are several challenges that remain to be addressed in the context of the secure end-to-end management and coordination of data. Furthermore, the EU General Data Protection Regulation (GDPR) gives more fine-grained control to the individual in use of personal data, and imposes more responsibilities on organizations. For individuals, when considering whether to share his/her data, it will be important that the data is shared with privacy and security in place. This will require an updated set of rights and obligations that addresses data portability, communication of data breaches to the data subject and transmitting data in a digital format.

Section 4. Cases

The paper will now present 5 cases from various countries, demonstrating attempts at creating some cohesion to personal/health data, with varying degrees of successes.

1. AUSTRALIA

My Health Record in Australia is the nation’s digital health record system\(^{35}\). It summarizes health information and data such as medical conditions, allergies, treatments, pathology and scan reports so that they can all be accessed through one system. Health information can be added by the patient, by healthcare providers and also imported from Medicare, which is Australia’s universal health scheme. As of 18 March 2018, over 5.5 million people were registered, translating to approximately 23% of Australia’s population.

The benefits of this digital health record system are themed around:

- **Better Access** – information can be accessed from any computer or personal device, and data goes with you if you move or travel interstate.
- **Improved Safety** – health providers can view your health information in a medical emergency.
- **More Convenient** – patients do not need to recall every detail of their health history
- **Strong Security** – patients can restrict who can view their health information
- **Privacy Matters** – hefty penalties for those who breach privacy measures.

However, several obstacles continue to challenge this system, which has cost taxpayers over $A1.2 billion dollars\(^{36}\). For example, presently coverage needs to improve, as it is not widely adopted by health professionals. Only 40 pathology and diagnostic imaging services were registered in March 2018, and 799 public hospitals and health services nationwide\(^{36}\). Another major hurdle is digital and reading literacy. Research into Australia’s Digital Divide has shown certain groups such as those living with disability, Indigenous Australians, and Australians with low levels of income or education are significantly less digitally included\(^{37}\) and risk exclusion.

Lastly, My Health Record suffers from the same fundamental problem seen in most countries – a lack of broad interoperability. While My Health Record operates across different States and Territories in Australia, the platform does not sync with existing, well-developed local software used by GPs. This means doctors need to manually add information, while deriving little added benefit from the task. Nor does it sync with the myriad of hospital software in use, nor private companies that collect health-related behavioral data.

Much can be learned from the Australian experience. Furthermore, it highlights the fundamental need for an interoperable, portable framework for health data management, such as MyData.

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Partly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can I <strong>see</strong> my data?</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can I <strong>trail</strong> my data?</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Can I <strong>use</strong> my data?</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Is my all my data <strong>integrated</strong>?</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>


2. United Kingdom

A UK startup called DigiMe\(^3\) is an example of person centric data management that has gained traction over the last few years. The company describes its mission as “a world where data is controlled by people for their own benefit”. How does it achieve this?

Firstly, DigiMe integrates personal data from various sources, including public and private organizations. For example:

- **Social data** - social media
- **Financial data** - banks, credit cards, financial institutions
- **Fitness and health data** – steam data from wearables, as well as medication and health data from certified providers
- **Medical records** – currently working to sync with the Icelandic Health System
- **Music and entertainment data**

Importantly, DigiMe states that it does not see, touch or hold the data of its users. Data is not stored on their servers, but instead encrypted (to bank or military level) and stored on a personal cloud such as Google Drive or Dropbox. Data is only shared with others when users have provided explicit consent. As a business, it derives its profit from charging a postal fee to companies when the user consents to their data being shared.

By having a transparent, person centric model of personal data management, apps no longer compete to collect and hoard data, but rather they compete to demonstrate how they can create value for customers using this data. It can achieve this by accessing richer, more accurate data to which customers have explicitly consented. Another benefit is that it facilitates data privacy and protections for citizens, so companies can focus on generating value rather than meeting data regulatory compliance.

DigiMe has now partnered with Dattaca and are working with the Icelandic Directorate of Health, which will improve the completeness of health data. Some other partnerships include Swiss Re, Lenovo, Reon, Western Digital and fnac.

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Partly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can I see my data?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can I trail my data?</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Can I use my data?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is all my data integrated?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^3\) https://digi.me/
As global citizens are increasingly mobile, medical information needs to be communicated quickly and comprehensively across borders. In this context, Swiss MEDBANK is a company that develops technologies to improve the safety of individual patients. It aims to do so by improving the way physicians can access an individual’s health information during an emergency, all around the world.

Customers create a Med’Profile, which can be shared around the world in a few seconds, and in several languages. Up to date information on diagnoses and allergies can avoid complications and errors. Information is accessed securely from a computer, tablet or smartphone, and it is processed through two programs – the Med’Profile Web and the Med’Profile Card. The card, which is the size of a credit card, has a fingerprint reader and USB plug. In the event of an emergency and unconsciousness, health professionals gain access through the customer’s fingerprint. It is essentially like an International Health Passport.

Such an innovation empowers people with the ability to make their health data portable across nations through the USB function. While broad data interoperability remains an issue, Med’Profile appears to be focused more on the emergency setting where any information, be it on a pdf, is more useful than none at all. Furthermore, it requires either for customers to manually input health information themselves, or request that their doctors do so. This restricts its use to people who are more digitally literate, and also its application in chronic disease follow up, where completeness of health information is vital.

Finally, it remains unclear whether customers can restrict various levels of access to viewing their personal health information. This is not only important in the context of the upcoming GDPR, but also as Med’Profile partners with insurance companies.

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Partly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can I see my data?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can I trail my data?</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Can I use my data?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is all my data integrated?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

39 http://www.swissmedbank.com/#med-profile
4. SWEDEN

Hälsa för mig (Health for Me) is a portal set to be launched by the Swedish eHealth Authority\(^4\). Through personal accounts, citizens can store health data of their choice from their smartphones and/or wearables secured and long-term. By providing an overview and the option to collect and share data, Hälsa för mig aims to empower the Swedish citizens and enhance their engagement in their personal health. Only citizens hold the rights to add, collect and share data.

Furthermore, it is hoped that the portal will work with private app developers on creating new services for the Swedish citizens, provided that they choose to share their all or some of their data. Within the Nordic region, this is the furthest progress made by the State to attempt to integrate health data from both traditional clinical sources, but also the increasing pool of health-related behavioral data.

The Hälsa för mig portal is currently undergoing a legislative investigation, as the original trial version was not approved by the Swedish Data Protection Authority. Updates are regularly posted on Hälsa för mig’s website.

![Hälsa för mig functionality](image)

<table>
<thead>
<tr>
<th>Can I see my data?</th>
<th>Yes</th>
<th>No</th>
<th>Partly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can I trail my data?</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Can I use my data?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is all my data integrated?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Hypothetically, as Hälsa för mig has not been launched

\(^4\) https://www.halsaformig.se/
5. FINLAND

Finnish citizens over 18 years age access their health records through the My Kanta Pages, a nationwide system incorporating data from public, private and occupational health care services. Login occurs safely using a bank log-in, an electronic ID card or mobile certificate. Citizens can view their electronic prescriptions, medical records, as well as manage their consents and refusals.

- **Electronic prescriptions:** these are shown for 2.5 years from the date of issue. It includes details such as drug purchases and which institutions have been involved with the prescription.
- **Medical records:** includes details on outpatient visits, medical records, summaries, diagnoses, critical risk information as well as lab tests and diagnostic imaging. This information is entered into the Patient Data Repository. The patient can identify incorrect information, but in order to edit this they still need to contact the health care service responsible for recording the data.
- **Consents and refusals:** patients have the ability to provide or deny consent to their health records being seen by health care units outside the original institution that recorded it. This is managed on the My Kanta Pages.

The benefits of a nation-wide Patient Data Repository include:
- Avoids repeating tests and procedures
- Improved flow of clinical information, which also enables patients to choose their location of care if necessary.
- Easier for the patient to keep track and monitor their own health information
- Health information is up to date.
- Consent is more transparent and easier to fulfill

**New Plans for 2018**

The My Kanta Personal Health Record (Kanta PHR) is a service under development in Finland that is scheduled to deploy its first phase in Spring 2018. It is voluntary, and will serve as a national data repository where citizens can enter information regarding their health and wellbeing. This may include vital signs, lifestyle and activity records that both directly and indirectly relate to their health. From the perspective of service providers, they must receive consent from the citizen as well as professional application authorized, which refers to a certified Class A social and healthcare data systems.

It is aimed that the PHR will be able to support the decision-making and diagnostic process concerning the health and wellbeing of Finnish citizens. Just like with the Patient Data Repository, citizens will have the right to withdraw consent at any time, through the My Kanta Pages.

---

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Partly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can I see my data?</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can I trail my data?</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Can I use my data?</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Is all my data integrated?</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

---

41 http://www.kanta.fi/en/omakanta
42 http://www.kanta.fi/en/web/ammattilaisille/omatietovaranto
Section 5. New Opportunities

A Model Case - My Nordic Health Record Card (NHRC)

The 2018 Swedish Presidency of the Nordic Council of Ministers set the agenda for an inclusive, sustainable, innovative and secure Nordic region, while recognising digitalisation as a recurrent theme\(^{43}\). Moving forward, one could ask – is it then possible to imagine a common Nordic Health Information Portal? If so, how would it look? How should such a model, which crosses national boundaries and languages, function within a network of separate institutions? Furthermore, can we learn from the wealth of digital knowledge that already exists within the Nordic region?

This white paper will now present a future scenario using a model case called the My Nordic Health Record Card (NHRC). The purpose of this model case is not to list a step-by-step instructional guide on how to build a common Nordic health data management portal. Rather, it should serve to inspire Nordic stakeholders with the knowledge, motivation and creativity to collaborate towards a common goal - a human-centric data management model that benefits Nordic citizens, societies and businesses. This will naturally be an iterative process that draws input and modification from healthcare professionals, the academic community, citizen associations, policy makers, businesses and ethicists, followed by refinement through public debate.

Opportunities

This paper will explore some of the opportunities and benefits that arise from a My Nordic Health Record Card. Opportunities will be presented for the patient, for society and for businesses operating in the Nordic region, summarised in Figure 6.

---

Patient

Figure 7 describes how Ingrid, a hypothetical patient from Sweden, experiences her diabetes management under a My Nordic Health Record Card. It describes how the NMRC can benefit her across several stages of her care including diagnosis, treatment, emergencies, research and even to help other Nordic citizens.

The NHRC, which takes the form of a physical card, is linked to an online platform where her medical reports, X-rays and prescriptions are stored in a digitally interoperable format, not simply in a scanned PDF. Further information such as emergency contact numbers, organ donation directives, allergies and blood type are easily sourced. With her permission, or in the event of an emergency, this information is accessible to all hospitals and healthcare professionals in the Nordic countries. The language of instruction is in English, with options to translate into Norwegian, Swedish, Danish, Finnish or Icelandic. If she wishes to seek medical treatment in any Nordic country, due to personal choice or by accident, her data is portable and interoperable.

On this health portal, the level of access is stratified into 3 levels of increasing restriction.

- **Level 3** only allows others to view the information, but no modification rights. This may be suitable for next of kin, or public health researchers. The extent of medical data that is viewable to researchers is specific to the relevant research question.

- **Level 2** allows others to view the information, but also to add and edit content. This may be appropriate for healthcare professionals involved in her direct care. If Level 2 clearance has been accessed during an emergency, without patient consent, it will be clear who has accessed the data, and the extent of viewing, so that there is transparency for the patient in the future.

- **Level 1** access is reserved for the patient, who can view, add and edit content, as well as grant consent for data to be shared with certain institutions or organisations. Any information that is edited by the individual patient would be shown in a different colour, to clearly differentiate between what has been written by healthcare professionals and that by the patient.

**Dynamic Consent**

Consent is one of the central features in this online portal. Private companies must seek explicit consent from individuals, through clear procedures and with the provision of user-friendly documents that explain the scope of use of health data. If the scope expands or changes, patients can be updated real-time with new consent solicited through the portal. Patients could either approve or withdraw consent at this point.
This raises the concept of **dynamic consent**⁴⁴, defined as a “personalised, communication interface to enable greater participant engagement in clinical and research activities”. It is dynamic because “it allows interactions over time”. It is a tool that was borne out of the perceived shortcomings in existing informed consent processes where participants were agreeing to future research use that was yet undetermined (eg. biobanking).

Dynamic consent has several benefits and the process can be made much easier through a common, interoperable Nordic health portal such as a My Nordic Health Record Card. Firstly, it recognises that consent is an iterative and not static condition, subject to changes in circumstances and personal beliefs. By providing patients with greater nuance, for example, the ability to withdraw from parts but not all of a research project, it encourages greater involvement public health research. Dynamic consent also establishes an ongoing relationship between patient and researcher/data scientist, through iterative notifications, queries and updates on research outcomes. Not only does this increase transparency, it also satisfies the patient’s reasonable curiosity as to how their health data has contributed to science.

As a Nordic citizen, Ingrid is able to receive medical treatment, fill prescriptions, integrate health and health-related data and communicate in detail with healthcare professionals across the Nordic countries. Her data is portable, reducing time inefficiencies and physical duplication, and her data privacy is preserved through a process of dynamic consent. Her tiered level of access to health data ensures that only necessary information is viewed by the appropriate people. However, how would this system benefit the Nordic societies, who presumably finance this new infrastructure?

<table>
<thead>
<tr>
<th>Access &amp; Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is a need to be able to look at and to compare data. Trusted models are needed for both individuals and institutions. A question is distinguishing between access versus sharing of data. The distinction being that with access a third party will look at your data through an access point, while sharing implies that they get your data. The functionality of both approaches have to be considered – but with the rapid technological development it is hard to state what is possible or not in the near future.</td>
</tr>
</tbody>
</table>

**Society**

Today digital health sits high on the Nordic political agenda. Telemedicine and ePrescriptions are slated to provide remote solutions to rural communities, fulfilling the Nordic Council’s goal of creating more inclusive and innovative societies⁴⁵. Alongside high levels of social trust, a window of opportunity has emerged. It is now possible to imagine the formation of this interoperable, unified Nordic health record that places Nordic citizens in control of their own healthcare data.

As the paradigm of precision medicine and health take hold, data will be the engine of this new vehicle. Innovative and exportable health data management models will be highly sought after internationally. However, on their own the Nordic countries are small, raising doubts about the scalability of such technological solutions. Therefore, combined regional expertise would solidify the Nordic’s position as a thought leader at the intersection of health and data science.

Using pre-existing Nordic health data registries, the vertical applications and benefits from this data are obvious (ie. answering the question that the data was initially collected for). Where the challenge lies is with the horizontal use of data points (ie. answering questions that the data was not collected for, but for which the data holds useful information). Comparative analysis of health data sets between municipalities, regions, and between nations, adds greater value. As the analytic capabilities of big data grow with time, this helps to build the evidence base for Nordic public health interventions. On an institutional level, medical treatments and clinical research would benefit from the interoperability of data sets, so that hospitals in Denmark can learn from those in Sweden, Finland, Norway and Iceland. For example, predictive modelling data on rates of early re-hospitalisation can reduce waste from inappropriate discharge⁴⁶.

Moving from a treatment focused health paradigm to one of prevention and early detection also brings economic benefits to Nordic societies. Less healthcare expenditure is spent on expensive hospitalisation, recurrent treatment of chronic diseases, as well as quality adjusted years of life (QALY) lost from the workforce⁴⁷⁴⁸.  

---


Finally, the value of preserving social trust in the Nordic region must not be understated. A 2018 report by the Nordic Council of Ministers recognised that trust in public institutions “underlies the fundamental values of equality, sustainability and co-operation”49. Despite this, governments will find social trust being tested and undermined if personal data flow remains ambiguous. This may be particularly the case as citizens become more aware of the extent to which their data is currently used. On the contrary, a MyData infrastructure empowers individuals with data rights and prevents the erosion of social trust, preserving the social and economic functions of Nordic societies.

**Business Opportunities**

Transitioning to a MyData-based infrastructure can also bring many benefits to businesses in the Nordic region. The first point to highlight is that transparency of data flow is necessary for open collaboration. Businesses, including pharmaceutical companies, increasingly need to adjust their business models to changing consumer patterns, growing knowledge complexity and the hyperspecialisation of medicine. It is no longer possible to undertake all activities ‘in-house’, therefore collaboration with academic institutions and crowd-sourcing knowledge becomes vital. Yet, the term open collaboration will remain a fancy word unless data rights and knowledge ownership are made more transparent. Secrecy hampers collaboration, which stifles true innovation in the private healthcare sector. As citizens become more aware of their data rights, governments will likely respond with stricter regulations as evidenced by GDPR. Businesses that encourage data transparency may be rewarded with participation, and participation sustains the long-term viability of these businesses.

Another opportunity for industry in the Nordic region will be the rise of new services in response to healthcare digitalisation. For instance, who will build and maintain these MyData health portals? Infrastructure maintenance including technical assistance, cybersecurity, data protection, processors and compliance officers will provide scope for new business opportunities in the Nordics. Furthermore, the current gap in baseline digital literacy will mean new opportunities for data counselling could emerge. Many citizens will need services that increase their knowledge of data and technology to navigate through a Nordic health portal. The public sector will likely struggle to keep pace with this volume, making way for private companies to offer this service.

Thirdly, the demand for efficacy and cost-effectiveness data of new digital interventions will likely pressure private healthcare companies to collaborate with health professionals. The emergence of various digital behaviour interventions and self-management apps have triggered greater scrutiny over their ability to deliver what they claim. This will be difficult in the current fragmented model of data management. Data aggregators hold onto data, locking out other businesses from entering the market. And without evidence of efficacy and cost-effectiveness, businesses will struggle with buy-in from health professionals and policy makers. By having a person centric, interoperable model of health data management, small businesses will have the opportunity to seek and integrate various types of health data. This will generate evidence to drive change in practice and policy that favours their product or service.

Finally, the emergence of public-private-crowd partnerships will demand a new framework for interaction between these stakeholders. Research has shown that public health communities are increasingly aware that they cannot act alone in tackling the commercial determinants of health50. Nevertheless, clarity will be needed on how to set common goals so that certain agendas do not dominate the partnership. Research work from Buse et al51 suggest clarity around the following criteria:

1. Setting appropriate targets
2. Independent monitoring
3. Transparent reporting
4. Sufficient scope for impact

For Nordic governments, the new terms of reference will influence the likelihood that citizens contribute their personal health data to businesses.

---

Emerging role: Digital Health Navigators?

With significant growth in the amount of health data collected and shared, several new uses of data can be expected in the form of new services, solutions or treatments. Figure 8 is a diagram lifted from a WHO bulletin depicting the growing complexity of the health data ecosystem\(^2\). In a context where the individual primarily or completely holds the rights to share their health data, as suggested by the MyData movement, the responsibility also falls back on the individual; individuals who actively share their data are more likely to receive a solution to their health demands.

Additionally, beyond access alone, this model would require the individual to know who to contact and which program is relevant for them. The data will naturally be stored digitally, which may create a gap between individuals proficient at accessing and sharing their data compared to those who are not. As indicated by research in Australia coinciding with the My Health Record, certain groups particularly with lower socio-economic status and disability tend to be digitally excluded\(^3\). How would we avoid the systemic exclusion of specific groups?

With this in mind, a potential emerging field is that of health navigation. Currently, the private, Swedish insurance company Skandia offers such a service. It is presently restricted mostly to cases of stress, however the concept could be expanded to also include usage and sharing of digital health data with relevant actors in the scenario above. This provides opportunities for both private businesses, as well as municipalities, to step in. Nevertheless, the challenge remains to ensure those who need counseling actually seek it, and how to proceed if the recommended treatment based on the individual’s data is too costly.

\(^2\) http://www.who.int/health/resources/ecosystem.pdf?ua=1

Figure 8: This diagram was developed by the World Health Organization, published in an article by Vayena et al titled Policy implications of big data in the health sector.
Section 6. Ethical Issues in a new paradigm

In a person centric model of health data management, new consequences and ethical challenges would arise. These are worth expanding on in the next section. Some obvious concerns regarding data privacy, storage and access are partly addressed by the GDPR, but still require further technical solutions on the implementation side. However, this paper identifies some broader ethical dilemmas emerging from a MyData ecosystem. We will focus on six broad themes.

From reading this section, it will become apparent that more challenges await in the horizon. During times of intense change, one may ask if it is better to do nothing at all. Yet in the current state of affairs, major ICT companies like Facebook, Google, Apple and Amazon have already accumulated large quantities of data. Commercial products and services based on people’s behaviour exist in the market today. In that sense, reality has already surpassed public moralisation of centralised vs decentralised health data models. Inaction, therefore, is not an ode to the past but rather an action itself that carries the weight of its own technical and ethical repercussions.
1. Selling vs. Sharing data
Selling is not the same as sharing. For instance, in countries where blood donation is paid, the pool of donors is skewed towards the poor and socially disadvantaged. This opens up the potential for exploitation, especially since digital data can easily cross international boundaries. Furthermore, donors may be dishonest about their medical history to sell inaccurate health data, as seen with HIV and blood donation. On the other hand, financial incentives can be powerful drivers of innovation in health. An example is PatientsLikeMe, a for-profit organization that connects patients diagnosed with rarer diseases. It sustains itself financially by selling anonymised data to research institutes and private companies. Unsurprisingly, it carries its own ethical challenges, such as covert patient exploitation and privacy breaches.

2. The Me in We
Rights and responsibilities are two sides to the same coin. If individuals benefit from public health interventions that are based on population data, what do we do about freeloaders? Should people be allowed to deny consent of their anonymised health data to public health institutions? This dilemma recognises that public health ethics can sometimes clash with an individual’s wishes. Utilitarianism is concerned with maximising benefit to the most number of people. In this context, it may justify infringing on individual liberties to achieve a common good. This is particularly relevant for Nordic countries, given its long tradition as a welfare state. If there is only me, and no we, in public health, the coherence of public health systems fall apart.

3. Winners and Losers
Any change to an ecosystem results in new power dynamics. Individuals do not start on an equal playing field. In this new future, those with high digital literacy will navigate through a health data portal with ease. Those less familiar with technology, be it through age or socioeconomic disadvantage, will struggle to fulfil their data rights. This not only impacts on usability, but also distributive social justice. The generalizability of precision medicine research is limited to those whose data has been included. For example, women and minorities have historically been excluded from certain aspects of medical research. Furthermore, information asymmetry means citizens will struggle to keep pace with businesses in the use and commercialisation of their health data.

4. Anonymity vs. Precision
As genomic, molecular and environmental data gets incorporated into clinical practice, a trend towards personalization emerges. It is a highly appealing narrative. We are all told we are unique. But how do you remain anonymous in the era of precision and individuality? Is this the only ethical value at play? It is important to consider the way in which current clinical research is conducted. In the gold standard of randomized control trials, individual variability is minimized so that apples are compared with apples. In the era of precision, not only does this challenge the future of medical research. It also demands for new ways to assess efficacy and cost-effectiveness, whilst minimizing bias. This is important for health policy and planning.

5. Nudging or Coercion?
As the amount of behavioral data on us grows it exposes uncomfortable questions about potential exploitation. Most agree that the state has a responsibility to encourage healthy eating & lifestyle behaviors, especially since healthcare is publicly funded in the Nordics. Despite good intentions, however, behavioral change interventions and behavioral public policy have the potential to slide from persuasion to encouragement to outright coercion. Furthermore, some may be concerned about the ability of governments to always prioritize citizens’ best interests. These questions are also relevant for private industries. While explicit consent can make data flow more transparent, it doesn’t prevent private companies from purchasing health data and exploiting it for marketing purposes.

6. Precision Medicine or Health?
If we truly wish to transition from a health paradigm of treatment to prevention, an honest question about goal setting needs to be asked. Moving from rhetoric to outcomes, Nordic governments will be challenged in the coming decade to scrutinize their policies and funding models – how far do they encourage the collective use of health data? Do they improve medical treatments or prevent progression to illness? This represents both a cultural shift in patient perspectives and expectations, but also an economic necessity as national budgets strain under growing medical costs. Finally, one may also reflect on the limits of health data or data-driven health, particularly in the implementation of solutions to essentially social problems. Loneliness, for example, is difficult to measure with data, and yet more difficult to solve using data.
Section 7. Future Game Changers

Blockchain technology
Apart from storage, centralisation of digital health data has also served the purpose of data security and accountability. For a proper transition to a person centric model of health data management, end-users (i.e. citizens) will need to be reassured that their health data is secure and that it can be validated without a centralised actor. Thus, a trustworthy ledger that accurately records previous episodes of access is greatly needed. However, current technologies that underpin the health data infrastructure of most countries do not satisfy these requirements. To the contrary, numerous instances of hacking and breaches in privacy have unsettled citizens and eroded trust. This vulnerability potentially threatens the ability to implement a person centric approach to health data management.

A promising area of development in this domain is Blockchain technology\textsuperscript{54} and similar derivatives. It refers to an open, distributed ledger that records transactions between two separate parties, in a manner that is both permanent and verifiable. The ability of Blockchain technology to embed transactions in digital code, protected from unauthorised tampering, deletion and editing, fosters transparency between all parties. It also raises the possibility of minimising intermediaries such as lawyers and brokers. Despite this, current Blockchain technology will struggle to sustain a MyData-based infrastructure of health data management, primarily for three reasons. Firstly, the energy consumption that is required for each transaction will be prohibitive as complexity and volume grows. Secondly, micropayments are embedded in each transaction, which will be a financial barrier to a portal that is operated by all Nordic citizens. Finally, scalability will be hampered by the time required to authenticate each transaction.

In this context, next generation Blockchain such as IOTA\textsuperscript{55} may hold promise. Using a Tangle ledger rather than blocks, this technology claims to settle transactions without mandatory fees or micropayments, while preserving the benefits of ledger technology seen in Blockchain. Furthermore, it claims to be scalable and lightweight, with much reduced energy requirements compared to its predecessor.

The promise of ledger technology should spur the strategies of Nordic governments moving forward as data privacy, accountability and transparency dominate public expectations. Furthermore, as hype gets separated from reality, there will also be organisational, societal and governance barriers to overcome. As Harvard Business Review pointed out\textsuperscript{56}, this is partly because ledger technology is not merely ‘disruptive’ but ‘foundational’, meaning its adoption requires huge investments that enable fundamental changes in economic and social systems.

Big Data Analytics during the era of Artificial Intelligence
In recent years, the term ‘big data’ has infiltrated the lexicon of almost every field, not least in the healthcare domain. Among its proponents in healthcare, the opportunities from big data analytics range from predictive modelling and clinical decision support to public health surveillance and research. So what makes data become big, and is it necessary to coin a new term if it simply means more?\textsuperscript{57}

Generally when people talk about big data, they refer to the well described 4 V’s\textsuperscript{58}, which are:

- **Volume** - amount or scale of data
- **Variety** - diversity of data types and sources
- **Velocity** - speed of analysis of streaming data
- **Veracity** - uncertainty in quality (or truthfulness) of data

\textsuperscript{54} https://www.blockchain.com/
\textsuperscript{55} https://iota.org/
\textsuperscript{58} http://www.ibmbigdatahub.com/sites/default/files/infographic_file/4-Vs-of-big-data.jpg
In healthcare, big data can therefore be defined as “encompassing high volume, high diversity, biological, clinical, environmental and lifestyle information collected from single individuals to large cohorts, in relation to their health and wellness status, at one or several time points”\(^{59}\).

As healthcare data management models evolve, it will be possible to link data from national health registries, electronic health records from various institutions, and integrate health-related data from medical devices, wearable devices and sensors based on virtual reality. The ability to analyse health trends from non-traditional data sources, such as social media, has also been demonstrated from the use of Twitter as an early warning tool during the 2009 swine flu pandemic\(^{60}\). Another example occurred during the 2015 Zika virus outbreak, where researchers analysed online media reports to predict transmission dynamics and plan subsequent public health responses\(^{61}\).

**Big Data, Thick Data, Long Data, and Deep Data**

In order to get an understanding of the differences and correlations between the data sets, Figure 10 describes the commonly known four different data sets briefly\(^{64}\). Big Data is defined as quantitative data at a large scale that involves new technologies around capturing, storing, and analysing. To be analysable, it must be normalized, standardized, defined, and clustered.

Deep and Long Data are mainly based on information from Big Data pools. Deep Data is taking massive amounts of data that is generated on a daily basis and transforms it with the insights from industry experts into useful sections, thereby excluding irrelevant information. Whereas Long Data are datasets of long timescales. They help to make correlations and understand how and in which pace human’s behaviours and decisions are changing over time. With this information, future trends can be anticipated.

In opposition to Big Data stands Thick Data, which is based on qualitative, ethnographic research methods. The aim is to show insights of the everyday lives of users/customers/patients etc. In short, it is a tool “for developing hypotheses about why people behave in certain ways.” The sample size is small, but the depth of livelong stories bring valuable insights that quantitative numbers cannot provide.\(^{62}\)

\(^60\) http://blogs.oii.ox.ac.uk/policy/can-twitter-provide-an-early-warning-function-for-the-next-flu-pandemic/
\(^62\) https://www.wsj.com/articles/the-power-of-thick-data-1395444914
<table>
<thead>
<tr>
<th>Big Data</th>
<th>Thick Data</th>
<th>Deep Data</th>
<th>Long Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reveals insights with a particular range of quantitative data points</td>
<td>Reveals the social context of connections between data points</td>
<td>Can help to predict industry trends or changes</td>
<td>Prevents missing out on important longer-term changes in the world</td>
</tr>
<tr>
<td>Relies on machine learning</td>
<td>Relies on human learning</td>
<td>Support in decision making processes, such as investments or reductions</td>
<td>It provides CONTEXT for fast and long-lasting changes</td>
</tr>
<tr>
<td>Isolates variables to identify patterns</td>
<td>Accepts irreducible complexity</td>
<td>Trial participant searches can be more streamlined and increase accuracy and efficacy of e.g. drug or treatment trials</td>
<td>Indicates correlations</td>
</tr>
<tr>
<td>Loses resolution</td>
<td>Loses scales</td>
<td>Improves accuracy by targeting individual pieces of information and specific trends</td>
<td>Focuses on target group analyses</td>
</tr>
</tbody>
</table>

The danger is when only relying on quantitative and optimised data, the humanitarian side gets lost and people, stories, and experiences are forgotten. More numbers do not necessarily produce more insights.

Best practice to uncover unknown territory, and to provoke inspiration. In order to realise the full potential of Big Data, Thick Data is needed to stay human-centered. Stakeholders and customers respond to emotions and stories, not numbers.

Whereas Big Data collects everything, Deep Data looks at specific information to help predict trends.

Big Data puts slices of knowledge in context, but to understand the big picture, the phenomenon has to be placed in its longer, more historical context.

The best solution for most businesses is a mixed methods approach where all forms of data analyses are used. The focus will change depending on the industry and target group.

This table shows the features of all four data sets and explains the value Thick Data, Deep Data, and Long Data can add to Big Data. Most businesses would profit from a mixed methods approach in which their data is analysed in a quantitative (Big Data), qualitative (Thick Data), analytical (Deep Data), and contextual (Long Data) approach.

**Big Data, Big Error?**

The different perspectives that thick, deep and long data bring to Big Data will be important when sifting through all the background noise, to separate true signals from false correlations. Therefore it is worth reflecting on the difference between precision and accuracy. The difference here is between measuring something right versus measuring the right thing.

![Accuracy vs Precision](image)

*Figure 10: Accuracy vs Precision*
3. Value-Based Healthcare

In recent years, much interest has focused on how health systems around the world can transition from a reactive, episodic 'fee for service' model towards one that provides value for patients, societies and businesses. While one solution to growing healthcare costs is simply to spend more money, affordable does not necessarily mean valuable. This distinction is particularly relevant in the face of a growing burden of non-communicable diseases. These chronic diseases are not, by nature, managed best through discrete, episodic interventions but rather through holistic and integrated care.

Despite this, many European countries face challenges in implementing such a system, not least due to varying opinions of what constitutes 'value'. Of course, this will depend on whose perspective is taken, be it the payer, the clinician, the caregiver or the patient. Further yet, value can be measured through traditional economic means, or by determining benefit in terms of social value or even ethical standards. At the heart of this tension is a question about how limited resources can be best allocated so that patients derive the greatest value and health benefits.

A basic condition for value-based healthcare to flourish is the ability to accurately measure outcomes, to reward services that provide most value and also to hold stakeholders accountable for what they promise to deliver. The definition of outcomes, and how they are measured, will therefore be vital. Furthermore, this will grow in complexity as we recognise the benefits of good health do not apply strictly to health alone, but span many social domains.

Value-based pricing for pharmaceuticals is an example of how insurance companies in the USA today are adopting a value-based approach to re-imbursement. Here, payments are linked with the delivery of a specified health outcome, rather than simply the prescription of the drug. A report released by Deloitte Centre for Health Solutions summarises the implications of this transition from volume to value. In order for value-based health to be fully achieved, accurate data on outcomes needs to be collected, analysed and delivered in a timely manner. A person centric model of health data management, along with clear rules on consent, facilitates the use of this otherwise untapped data.

---


---

Figure 12: Components of value-based health care. Information source: https://www.isc.hbs.edu/health-care/vbhcld/pages/default.aspx
4. International Health Account Number (IHAN)

Finland has decided to embrace the opportunities with GDPR and actively adopts MyData principles in their strategy. One example currently under development is IHAN® – an international account system for data exchange that uses the IBAN bank system as inspiration. Initiated and in development by SITRA in Finland, IHAN builds on the new reality with GDPR and uses decentralized MyData concepts as its vision. The IHAN model recognizes each person in relation to his/her personal data just as IBAN recognizes each bank account. Put simply, it can be described as a dynamic data donor system where the individual controls and decides the use of their own personal data – which opens up whole new ways of secondary use of personal data.

**IHAN® Principles**

- Consumers can control all data collected by themselves (based on legislation)
- Consumer may have many virtual identity and manage them all with their freely available data management console software
- Data existence will be registered and access to data usage have to be authorized
- Service providers and data holders will allow access to consumer’s data based on his or her consent or order
- Service providers and data holders are obligated to allow data transfer to a consumer itself or 3rd party by an order from a consumer
- Service providers and data holders will use IHAN® Logo to proof their commitment to IHAN®

<table>
<thead>
<tr>
<th>International Bank Account Number (IBAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This refers to an internationally agreed system to identify bank accounts around the world. It consists of a number that is attached to all bank accounts in most European countries. Data exchange can also greatly benefit from such a system.</td>
</tr>
<tr>
<td><strong>IBAN:</strong> FI 50 0004 00440116233</td>
</tr>
<tr>
<td>Maximum 34 alphanumerical characters</td>
</tr>
<tr>
<td>▪ 2 letters to indicate home country (e.g. FI)</td>
</tr>
<tr>
<td>▪ 2 numbers are a control key</td>
</tr>
<tr>
<td>▪ Remaining characters identify the bank and ordinary bank account.</td>
</tr>
<tr>
<td>The benefits of this system include:</td>
</tr>
<tr>
<td>1. Standardization</td>
</tr>
<tr>
<td>2. Verification</td>
</tr>
<tr>
<td>3. Protection</td>
</tr>
<tr>
<td>4. Speed</td>
</tr>
<tr>
<td>5. Facilitates cross border transactions</td>
</tr>
</tbody>
</table>

IHAN and similar concepts build on existing frameworks such as X-road, which is the data exchange standard in public sectors of Estonia. The key value behind X-road is interoperability, which enables the integration of data from different public and private organizations and information systems. As described on their website, “all outgoing data from X-road is digitally signed and encrypted, and all incoming data is authenticated and logged”. The functionality of X-road is estimated to save Estonians 800 years of working time per year. The success from X-road has spurred development and implementation in Finland, Faroe Islands, Azerbaijan and Namibia.

---

Section 8. Recommendations and Roadmap

1. Conduct an in-depth comparative analysis of the differences in Health Information Portals in the Nordic countries today, including an analysis of governance structures within the health systems. Identify areas that need alignment.
   i. Define the role of public sector health data aggregation, and how this will be enforced following the decentralizing of health data.
2. Define good data practices for data access and data sharing, including the status today.
   i. Identify the most appropriate measures, indicators and assessment tools for efficient and trusted data sharing principles, to develop a mature model for data practice in the Nordics.
3. Exploit enabling technologies
   i. Define the dynamics between individual, secondary and third party use of health data.
   ii. Investigate novel data management possibilities, including dynamic consent.
   iii. Explore the potential benefits of Blockchain-like technology (distributed ledgers) in the implementation of person centric health data management.
4. Provide a more detailed analysis of key ethical challenges regarding data management in the future.
5. Establish a co-operation: Identify and engage key stakeholders in the digital health revolution.
   i. Conduct public forums in key Nordic cities.
   ii. Align the Nordic regional ambitions with the EU agenda, especially the upcoming GDPR regulations, Digital Single Market and eHealth strategy.
   iii. Ensure political alignment among Nordic countries when specifying a strategic agenda towards a person centric model of health data management, based on MyData principles. The MyData Local Hubs should be used, as well as meetings and conferences.
6. Business potential: Articulate business opportunities that arise from a person centric model of health data management. Engage with private companies to determine their needs and facilitate the development of sustainable business models.
7. Learning points:
   i. Explore the potential learning points from the Estonian-Finnish experience with implementing X-road.
   ii. Explore IHAN as a component of person centric data management, with regards to integrating health and health relevant data.

Roadmap 2018-2020

Figure 13: Roadmap for the next 3 years
Conclusion

The future of health and medicine will undoubtedly merge with digitalisation and data. This might seem like an inevitable evolution of the fields, but many aspects remain open for adjustment. For instance, which technologies can sustainably facilitate the flow of health data? How will the growing volume of behavioural data be integrated appropriately with clinical data? What kind of partnerships will governments and businesses create to utilise health data for public benefit? The answers to these questions are hardly set in stone, but one thing is certain. The way in which health data is managed, as well ownership and control of this data, will drive the terms for future negotiations.

Opportunities do not present themselves twice during these large-scale transitions. Nordic countries sit in a unique position of having high levels of social trust, collective-oriented mindset of public good, and pre-existing digital infrastructure and literacy from longstanding population registries. Meanwhile, citizens increasingly recognise the need for more transparency, and this is mirrored by upcoming GDPR regulations to sweep across Europe. Early investment on person centric health data management today will provide benefits to Nordic individuals, societies and businesses in the region.

Political, economic, societal and institutional agendas will need to align. As the Nordic Council of Ministers converge to discuss strategies for the future of the region, it can begin by exploring the merits of person centric health data management. Failure to capitalise on this opportunity and Nordic countries may soon find themselves eclipsed by a situation in which private data aggregators, or other nations, dictate data priorities for Nordic citizens. With the arrival of GDPR, MyData begins to construct a frame to handle the new digital reality, in order to create more value from data by setting it free.