TOWARD AN INTEGRATED HEALTH INFORMATION SYSTEM IN THE NETHERLANDS

DRAFT INTERIM BRIEF AND RECOMMENDATIONS

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Acknowledgements

This interim policy brief is part of a series of country reviews of health information systems that was launched by the OECD Working Party on Health Care Quality and Outcomes (HCQO) and is part of the 2021/22 programme of work of the OECD Health Committee. The OECD thanks the experts within the Netherlands that gave of their time to participate in interviews and focus groups. The OECD acknowledges Herko Coomans for his support in coordinating the study in the Netherlands. The brief was authored by Jillian Oderkirk and Luke Slawomirski with input and guidance from Niek Klazinga, David Morgan and Michael van den Berg and assistance from Duniya Dedeyn. Thanks are extended to Francesca Colombo and Frederico Guanais for their comments on a preliminary draft.

Table of contents

Tables

Figures

Boxes

Executive summary and recommendations

Health systems of the 21st century will be built around information: the right information reaching the right person at the right time. In the Netherlands there are separate discussions and initiatives about the interoperability of clinical data for direct patient care, the exchange of health data to develop health care quality measurement, the development of personal health environments, and the creation of research infrastructures for the life and social sciences.

There is not yet, however, a coordinated national effort toward an integrated health information system that could efficiently modernise patient experiences, support integrated health care delivery, improve monitoring of public health, support evidence-based policy making, and encourage innovations in health technologies and advancements in research.

In January 2021, the Ministry of Health, Welfare and Sport of The Netherlands commissioned the OECD to gather evidence and recommend legal, policy and organisational reforms to transform the existing arrangements into an integrated information system that supports the government in achieving four key goals:

1. Strengthening integrated health care delivery across settings and sectors
2. Enabling comprehensive public health monitoring and management
3. Capitalising on recent innovations in health information infrastructure
4. Fostering research and innovation in technologies and treatments that improve health and health care.

To understand the strengths and weaknesses of the current health information system and to develop recommendations, the OECD, through a series of focus groups and interviews, consulted national experts from academia, business, and government regarding the Netherlands' health information system in January to March of 2021. The information gathered through consultations with experts was complemented with information on the Netherlands and other OECD countries that was gathered through the OECD's regular program of monitoring countries' health information systems.

This report describes the current landscape of the Dutch health information system and recommends policy and organisational reforms to achieve an integrated health information system in the Netherlands.

This interim report will be followed in the Fall of 2021 with a full report from the OECD review of the health information system in the Netherlands. Further consultations with experts about these interim recommendations will be undertaken to support the final report.

Recommendations

The OECD recommends that the national government takes full responsibility and leadership for establishing a 21st Century, integrated health information system in the Netherlands that adheres to the FAIR principles, which means that all relevant data – including health care data as well as public health data and social care data are -- Findable, Accessible, Interoperable and Reusable.

The key objective is enabling comprehensive and consistent uses of health data for care delivery, for monitoring and improvement of quality and outcomes, for public health, for policy making, and for research and innovation.

An integrated health information system does not require radical structural reforms and can be achieved within the existing Dutch health system. The effort should capitalise on strengths including those of existing organisations; while addressing key gaps in leadership, policy, regulations and incentives that discourage collaboration, inhibit data exchange, impede the adoption of standards for data content, exchange and sharing, and limit research and innovation.

A useful analogy is an integrated transportation network, which allows passengers to move safely and securely across regional boundaries around the entire country, using various transport types, with an integrated ticketing system, timetable and journey planning.

Four key areas of policy and organisational reforms are recommended to achieve an integrated health information system:

1. Developing a National Strategy
2. Operationalising the strategy through a national agency
3. Governance, regulatory and policy reforms
4. Development of technical standards and infrastructure.

A national strategy

The Ministry of Health, Welfare and Sport would lead the development of a National Strategy for an integrated health information system. We recommend a unit is established within the Ministry that is staffed with a team of experts in health information, IT, data science and 'privacy-by-design'[1].

1. Information Council (IC) should advise the ministry on the strategy; and IC members should act as ambassadors and spokespersons for the strategy.
2. IC membership should expand to include representatives from all key stakeholders in an integrated health information system, including organisations with responsibility for national health information (including health care, public health and social care data); national health care quality registries; national health research infrastructures; and organisations providing national health data access, linkage and governance.
3. Public consultation at all stages of development of the national health data governance framework and public information, such as a website, to disseminate information about the development process and its outcome, as part of the National Strategy.
4. Consider a government campaign to change the mindset and culture around data sharing and exchange, with high profile spokespeople and champions. This is to:
    a. Assuage public and stakeholder concerns about privacy risks, and reassure how privacy can be protected when data are used
    b. Communicate the benefits of health data as a public good.

[1] Privacy by design is a term used to describe information technology design and engineering that incorporates privacy throughout the entire development process. Its seven principles are: Proactive not reactive; preventive not remedial; Privacy as the default setting; Privacy embedded into design; Full functionality – positive-sum, not zero-sum; End-to-end security – full lifecycle protection; Visibility and transparency – keep it open; and Respect for user privacy – keep it user-centric. See also Box 1.

Operationalising the strategy through a national agency

A national agency is needed to become a single central authority to implement the National Strategy to 'build the tracks'. This could be created by strengthening an existing organisation or creating a new organisation. This would comprise:

1. Agreeing (or developing) consistent national standards for
   a. Semantics (terminology)
   b. Electronic messaging (exchange)
   c. Data accessibility/sharing (prevent information blocking); and keeping the standards up to date.
2. Consulting with the IC and involving the IC in standards development and maintenance.
3. Formalising the role of the IC and its interconnection with the national agency.
4. Consulting with any stakeholder groups not represented within the IC, such as eHR systems and digital tool vendors.
5. Certifying vendors of IT solutions and digital tools for compliance with national standards.
6. Certifying and verifying health care providers and other information system actors have achieved interoperability standards and are exchanging useable data and not blocking data.
7. Ensuring that this agency operates under a formal shared governance of standard setting with the major health research infrastructure organisations and health information organisations, so that standards are fit for all data uses within the National Strategy.

Governance of the integrated health information system

The Ministry, advised by the IC, executes key policy and legal reforms to 'build the signals' and realise the National Strategy including:

1. Develop administrative orders to legally authorise and finance the National Strategy and the agency that implements the strategy. This should:
   a. Act as follow-on administrative orders to the draft framework legislation for data exchange via quality of care standards.
   b. Create the conditions for agreed national standards for health data terminology and exchange for direct care and secondary uses, including quality monitoring.
   c. Incorporate exchange of public health data and social care data.
   d. Formalise the role and mandate of the Information Council.
   e. Formalise the role and mandate of the national agency tasked to implement the national strategy.
2. Develop national guidelines for the implementation of the GDPR for stakeholders in the health information system, emphasising privacy-by-design,4 FAIR principles and reasonable approaches or lawful alternatives to consent.
3. Revise legacy legislations that are posing unnecessary obstacles to an integrated health information system.
4. Ensure national guidance aligns with existing and developing guidance and regulations at the European level.
5. Review and reform government subsidies/financing of stakeholders and projects in the health information system, including research projects funded by government grants, to create financial incentives for:
   a. Complying with national GDPR guidelines

   b. Complying with national data standards, and
   c. Demonstrating (verifiable) data interoperability.
6. Consider financial incentives to encourage health care providers and other actors in the information system to move to certified IT solutions and succeed in achieving verifiable interoperability.
7. Consider how the proposed funding and remuneration reforms that reward care coordination and value currently align with incentives to enable the exchange of healthcare, public health, and social care data.
8. Evaluate the functionality of the two funded data exchanges (LSP and MedMij), to harmonise toward a method for data exchange that meets the needs of all stakeholders and achieves the goals of the national strategy, including to ensure the data exchanged will cover all patients and all providers.
9. Consider how the proposed funding and remuneration reforms that reward care coordination and value currently align with incentives to enable the exchange of healthcare, public health, and social care data.
10. Evaluate the functionality of the two funded data exchanges (LSP and MedMij), to harmonise toward a method for data exchange that meets the needs of all stakeholders and achieves the goals of the national strategy, including to ensure the data exchanged will cover all patients and all providers.

Technical standards and infrastructure supporting the National Strategy

The national agency implementing the National Strategy should also:

1. Participate in global and European efforts to develop global standards for health data terminology and exchange.
2. Re-code data, where necessary, to a common health data model to support and facilitate information development/analytics. Prioritise leading global data models.
3. Prioritise use of modern IT architecture and global or European standards for data terminology and exchange (messaging).
4. Ensure standards comply with current and emerging European regulations and that the Netherlands can participate fully in multi-country European and Global research and monitoring.
5. Keep national standards up-to-date as technologies and data develop over time.

Review of the Dutch health information environment, landscape and ecosystem

The importance of an integrated health information system

The past decades have seen profound changes in health and health care. Not only are people's health needs and expectations now different, but the technologies at our disposal are opening new possibilities and frontiers.

Health systems of the 21st century will be built around information: the right information reaching the right person at the right time. This enables providing high-quality integrated care to all people in need, as well as better public health practice, health system management, and research and innovation. While health systems will continue to be structured, funded and organised differently, success – in terms of better care, public health, system management and research – will be characterised by a comprehensive, coherent, standardised and integrated approach to managing (electronic) health data.

An integrated health information system means that electronic data are FAIR (findable, accessible, interoperable, reusable), and can be exchanged and securely used by other actors and institutions that serve the public interest. The result is that information can flow, safely and securely, to where it can be used to advance human health and wellbeing.

Within the Netherlands there are separate discussions and initiatives about the interoperability of clinical data for direct patient care, the exchange of health data to develop health care quality measurement, the development of personal health environments, and the creation of research infrastructures for the life sciences and the social sciences.

There is not yet, however, a national effort toward an integrated health information system that could efficiently modernise patient experiences, support integrated health care delivery, improve monitoring of public health, support evidence-based policy making, and encourage innovations in health technologies and advancements in life sciences and social science research.

In January 2021, the Ministry of Health, Welfare and Sport of the Netherlands commissioned the OECD to gather evidence and recommend legal, policy and organisational reforms to support creating an integrated health information system to support four key national policy goals:

1. Strengthening integrated health care delivery across settings and sectors (so that an individual's relevant health information can be accessed by them as well as their providers ranging from first responders to general practitioners to hospitals and allied health providers)
2. Enabling comprehensive public health monitoring and management (including of the Covid-19 pandemic)
3. Capitalising on recent innovations in health information infrastructure

4. Fostering research and innovation in technologies and treatments that improve health and health care.

In simple terms, an integrated health information system enables the secure exchange and movement of organised and standardised 'health data' to where they can create valuable information and knowledge. Health data are data relevant to health and health care covering the entire population, and comprise data created and managed in the health care, public health, and social care sectors/settings. For the Netherlands this implies data on acute- and long-term health care as well as data on public health (publieke gezondheid) and social care (sociale domein) (Figure 1).

Figure 1. Three key types of data in an integrated health information system

Source: Authors.

A useful analogy is an integrated transportation network, which allows passengers to move safely and securely across regional boundaries around the entire country, using various transport types, with an integrated ticketing system, timetable and journey planning.

The importance of an integrated health information system has recently been highlighted in the Dutch media[2], which reported difficulties with transferring COVID-19 patients between hospitals because their medical information cannot be exchanged electronically. This results in not only delays and inefficiencies – with busy clinicians having to manually transcribe patients' data from the local electronic record to a CD to send with the patient – but also the risk of subsequent medical errors that manual transcribing of information entails.

An integrated health information system would help the Netherlands to not only directly improve care quality, outcomes and patient empowerment by enabling patients and their healthcare providers to access

[2] https://eenvandaag.avrotros.nl/item/gegevens-op-de-fax-of-een-dvd-bij-verplaatsing-van-coronapatienten-wordt-gemis-van-elektronisch-patientendossier-wel-heel-duidelijk/

health information, it would also raise the country's capacity to use these data for other important purposes including:

- Managing health system performance on national, regional and network level
- Public health monitoring and surveillance
- Opening new communications channels with patients to improve patient-centred care such as the active use of patient-reported metrics (PROMs and PREMs)
- Introduction of new digital services such as e-prescriptions or telehealth
- Better targeting of reimbursement for services to reward value
- Biomedical research and development
- Innovation such as big data analytics and artificial intelligence that will enhance knowledge-based decisions for patient care and health system governance.

Individual-level data are needed for both primary and secondary uses

The same data point should serve many uses, from informing a physician caring for a patient to helping patients manage their care, to health care quality monitoring indicators, value-based payments, real-world evaluation of the effectiveness of therapies and contributing to clinical decision support tools (artificial intelligence).

Recent advances in the latter mean that individuals' data are now used to inform decisions about their care and the care of others. The distinction between using data for primary purposes (direct patient care) and secondary purposes (e.g. research, public health monitoring) is therefore increasingly blurred.

For this reason, health data today cannot be easily categorised as personal or non-personal when the data pertain to individuals. A simple data processing step, such as removing personal identifying information like names, addresses, health insurance numbers and birth dates from a data set, does not yield anonymous data because it is increasingly easy to re-match the data to other datasets and re-identify individuals with some probability of success. More complex manipulations or aggregations of data to try to guarantee anonymity may destroy the quality, validity and usefulness of the data to produce valid information and research results.

Even the simple data processing step of removing personal identifying information must be carefully considered, as the linkage of datasets may require this information, for example to link hospital inpatients to mortality data to find out how many patients died in the weeks following a procedure. Mechanisms that allow re-identification for approved data uses, such as investing in pseudonymisation and secure storage of re-identification keys, are recommended by the OECD (see Annex C).

This review sets out to support the Netherlands in developing an integrated health information system that maximises data protection and data security, complies with EU GDPR requirements, and maximises the development, accessibility and usefulness of personal and non-personal health data to serve the public interest.

It should be stressed that an integrated health information system does not require all data to be stored in a single location. It is quite possible to achieve the above objectives without central storage or even aggregation. A unified and coordinated approach to national data governance can enable smooth information exchange and use for a range of purposes without compromising privacy, security and ownership of data. In fact, in some ways data protection can be enhanced under a federated data structure.

Further, ensuring that data can be exchanged across national borders into Europe and beyond can amplify the benefits of data analytics and research in, for example, the context of public health, rare diseases, pharmacovigilance, and precision medicine. An information system that follows international data standards facilitates within-country and cross-border healthcare delivery and business opportunities for the

Netherland's research and technology sectors; and is better prepared to participate in and adapt to European regulations and initiatives.

Development of interim recommendations

To understand the strengths and weaknesses of the current health information system and to develop recommendations, the OECD, through a series of focus groups and interviews, consulted national experts from academia, business, and government regarding the Netherlands' health information system in January to March of 2021 (See Annex A). The discussions focussed on three questions:

1. Health data interoperability (exchange and sharing): What are the challenges and what are the policy tools that can address them? i.e., regulations, incentives, standards, certification?
2. Personal health environment: What are the digital tools that deliver a modern health care experience, provide data access and allow interactivity?
3. Organisation and governance: What national institutions and governance mechanisms support a strong and trustworthy national health information system?

The information gathered through consultations with experts was complemented with information on the Netherlands and other OECD countries that was gathered through the OECD's regular program of monitoring countries' health information systems including a 2019-20 Survey of National Health Data Development, Use and Governance and a 2021 survey of Electronical Health Record System Development, Data Use and Governance.

This note is an interim output of the Review commissioned by the Ministry and it will be followed by a more detailed report, which will be published in late 2021. The remainder of this document comprises three sections.

- An overview of the current Dutch health information environment -- its strengths, weaknesses and opportunities for improvement (the 'now').
- An outline of the changes and approach required to create an integrated health information system that aligns with international trends and strategies (the 'what').
- A set of preliminary recommendations on instituting these reforms (the 'how).

The Dutch health information landscape reflects the organisation of the Dutch health system

The health and healthcare system of the Netherlands has traditionally performed very well in comparison to other OECD countries. But, in terms of its structure and design, the system is quite unique. It is built on principles of decentralisation, competition, market mechanisms, and the private (not-for profit) sector to deliver quality care to its citizens. A key feature has been to reduce the role of government in health care financing and delivery.

The result is a fragmented system, both geographically as well as across health settings and sectors – exemplified by the separate approaches toward managing and using public health data, health care data and social care data.

This is not unique, of course, but in contrast to other health systems where it is a result of either legacy factors or unintended policy consequences, fragmentation in the Netherlands is a *design feature*.

Fragmentation and the consequent high number of data custodians -- does not ipso facto impede nation-wide cooperation, coordination, and data standardisation, but it makes it indispensable to have coordinated, national policies, legislations, incentives, and governance mechanisms to support and

encourage actors toward the common goal of optimising the use of existing data. This section outlines where the Netherlands currently stands in this regard.

Several strengths and advantages will enable creating an integrated health information system

Netherlands performed well compared with OECD countries in many aspects of health data maturity, use and governance in a 2019-20 OECD survey. In most cases, the data needed to achieve the objectives outlined in the introduction exist. All that is needed are a set of consistent rules to connect actors in the information system together and to enable access to the right data by the right people at the right time.

Expert consultations revealed other strengths. For example, patient engagement and leadership of patient groups toward data interoperability is strong in the Netherlands. Significant progress has been made in developing data exchange standards. The Information Council (IC) has made good progress in advancing the case for data exchange for better care delivery, although the IC is a voluntary body with no legal status or funding and its membership and focus is limited to primary users and use of data.

In addition, the Netherlands has a unique 'can-do' culture with a strong tradition of finding solutions to seemingly intractable problems. This has often relied on striking a balance between individual liberty and the need for collective action (it is, after all, a country that manages to not only exist but thrive below sea level).

An example of local innovation in this context is the personal health train -- an important technology developed in the Netherlands, which can enable data exchange on a distributed/federated network thus avoiding the need for central aggregation of personal data (Health RI, 2021).

Radical health system reform is not needed

The Dutch health system has served the country very well in the 20th century. But the challenges and opportunities of the 21st century are vastly different and health data are becoming strategic assets if they can flow safely to where and when they are needed and are useable upon arrival.

Achieving this data flow is possible without changing the functioning or actors in the existing Dutch system, which operates based on competition, markets and minimal government involvement. With legal and policy reforms as well as modern digital technologies, existing actors in the health information system can be connected to new tracks that allow them to exchange data with one another; and where the users of these tracks follow common rules, as is the case for any vehicle using a public transportation network.

Building the tracks and the signals, to create an integrated health information system that meets the needs and opportunities of the 21st century will require national leadership, a strategy and a governance framework.

Data custodians in the Netherlands adopt different approaches to data governance and exchange

The Netherlands' health information system is characterised by the highest number of data custodians reported in the OECD. This fragmented structure does not preclude being able to leverage available data to achieve the objectives listed earlier. It does, however, create greater challenges to data sharing and integration than in other countries.

A 2019/20 OECD survey found that most OECD countries have 3 to 5 custodians of the thirteen national health and health care datasets considered integral to a national health information system. Custodians of

these data are usually national governmental organisations such as health ministries, national statistical offices or health information agencies funded by the government (Oderkirk, Survey Results: National Health Data Infrastructure and Governance, 2021).

The Netherlands reported nine separate custodians of key national data assets, with only one custodian being a fully governmental body, Statistics Netherlands (CBS). Most data custodians are either government-funded autonomous foundations or institutes, or private-sector funded non-profit organisations (Annex B Table 2).

Dutch health data custodians adopt different approaches to health data governance, including policies around data sharing and access to data for within-country and cross-border statistical and research projects (Annex B Table 3). Further, their adoption of best practices to protect privacy and data security, including 'privacy-by-design' varies (see Box 1 and Annex B Table 4).

Legislations, regulations and their interpretation can hinder data exchange

In their submission to the 2019-20 OECD survey, Dutch officials reported that organisations can create datasets and can undertake dataset linkages only if their proposed activities meet the requirements of the EU General Data Protection Regulation (GDPR) and the Medical Treatment Act. The Netherlands' Data Protection Authority evaluates whether datasets meet GDPR requirements.

However, without national health data governance guidelines for the implementation of the GDPR, officials reported that dataset custodians each have their own interpretation of the GDPR and that some have interpreted the GDPR as indicating that past data exchange arrangements are no longer legally permitted. For example, sharing data between custodians for the purpose of calculating indicators of health care outcomes by health care institution is often considered legally prohibited.

Privacy-protected data uses are supported by the GDPR but need to be implemented

Implementation of the GDPR can include national legislations regarding the collection, exchange, linkage and accessibility of health data and authorisation of data processing by a legal basis that is not limited to patient consent. Implementation guidelines for organisations processing health data are also necessary to avoid divergent interpretations that unnecessarily reduce data exchange and collaboration.

A recent preliminary opinion of European Data Protection Supervisor regarding the creation of a European Health Data Space (EHDS) explains that because the space will be created to enhance access to health data in order to allow for evidence-based policy decisions and for scientific research within the EU, they do not consider Article 6(1)(a) GDPR (i.e. consent of the data subject), as the most appropriate legal basis (EDPS, 2020). Instead, they refer to Article 6(1)e that authorises health data processing where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; Article 9(2)(i) that allows processing of sensitive data for reasons of public interest and Article 9(2)(j) that authorises processing operations involving health data when the processing is necessary for scientific research purposes. Further, they explain that Article 89 allows member states to develop legislation that provides for derogations from certain rights, subject to safeguards.

GDPR provisions may still provoke some limitations, however, such as the use of data for exploratory purposes including machine learning and AI algorithm development, which require greater volumes of data than principles of data minimisation may support (Hashiguchi TCO, Forthcoming). Another example is the use of blockchain technologies which can violate rights set out in the GDPR, such as the right to erasure (OECD, 2020). Resolving these issues will require further work at the European level but do not limit the Netherlands from adopting the recommendations set out in this report.

Box 1. Privacy-by-design and the OECD Council Recommendation on Health Data Governance

The Privacy-by-design approach involves designing IT systems in a way that pro-actively anticipates and addresses risks to data privacy and security so they may be mitigated. In such approaches, the privacy of all individuals whose data is within the system is protected by default. The protection of individuals' privacy and data security is embedded within the architecture and functionality of the IT system. At the same time, the IT system supports all uses and re-uses of data that are in the public interest.

Privacy-by-design is important because health data are often personal and sensitive, particularly health micro-data where there is a data record for each individual. The EU Data Protection Regulation (GDPR) [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016] places personal health data in a special category with the highest standards of protection.

The OECD Recommendation on Health Data Governance responds to the growing need for a consensus about the framework conditions within which health data can be appropriately governed to enable health data processing to take place both domestically and transnationally. Such health data governance frameworks require a whole of government approach; given that the public interests served span the domains of health, justice, industry, science, innovation and finance. The OECD Council Recommendation on Health Data Governance is compliant with the EU GDPR and encourages 'privacy-by-design'.

The OECD Recommendation on Health Data Governance was adopted by the OECD Council on 13 December 2016 and was welcomed by OECD Health Ministers at their meeting in Paris on 17 January 2017. The Recommendation provides policy guidance to:

- Encourage the availability and use of personal health information, to the extent that this enables significant improvements in health, health care quality and performance and, thereby, the development of healthy societies while, at the same time, continuing to promote and protect the fundamental values of privacy and individual liberties;
- Promote the use of personal health data for public policy objectives, while maintaining public trust and confidence that any risks to privacy and security are minimized and appropriately managed; and
- Support greater harmonisation among the health data governance frameworks of Adherents so that more countries can benefit from statistical and research uses of data in which there is a public interest, and so that more countries can participate in multi-country statistical and research projects, while protecting privacy and data security.

Governments adhering to the Recommendation will establish and implement a national health data governance framework to encourage the availability and use of personal health data to serve health-related public interest purposes while promoting the protection of privacy, personal health data and data security.

The Recommendation sets out twelve key elements of the development and implementation of national health data governance frameworks (See Annex C). The elements encourage greater cross-country harmonisation of data governance frameworks so that more countries can use health data for research, statistics and health care quality improvement.

Sources: OECD (2019), Recommendation of the Council on Health Data Governance, OECD Legal Instruments, Paris, http://legalinstruments.oecd.org; and Cavoukian A (2006), Privacy by Design: The Seven Foundational Principles.

The OECD Council Recommendation on Health Data Governance sets out the elements for a national health data governance framework and fosters a 'privacy-by-design' approach that is consistent with the EU GDPR requirements. Both a national health data governance framework and guidance on the implementation of the GDPR would help to overcome different legal interpretations that are limiting data sharing in the Netherlands. The framework would help to avoid the over-use of consent to authorise data exchange, in favour of legal authorisation and requirements for a 'privacy-by-design' approach that protects data privacy and security while enabling data to be exchanged and used for legitimate purposes.

A further issue raised by experts in the Netherlands are legacy legislations that precede the GDPR and that may create unnecessary obstacles to the exchange and use of health data. In particular, the Medical Treatment Contracts Act (Wgbo) requires doctors to obtain patient consent to share data with third parties. Third parties include quality standards/registers. Under Wgbo, patients are required to provide explicit consent for their records to be included within the national exchange point (LSP). As a result, the exchange is missing data on non-consenting patients and for patients whose health care provider did not ask them to provide consent. This limits the reliability of the data for direct care or secondary uses.

New framework law is a good start but will need follow-on administrative orders and policies to achieve the desired result

A new framework law introduced in 2021 aiming to improve health data interoperability takes a cautious and incremental approach, raising concerns among experts interviewed that full health data interoperability would not be achieved. Experts interviewed indicate that the law asks health care professionals to set standards for treatment. The standards are then submitted to the National Quality Register, which has a legal status. When the National Quality Register adopts the standard, it would become a norm that the Inspectorate has the authority to uphold. The Ministry would then 'translate' these professional standards into technical/informational requirements.

The framework law will likely require additional follow-on administrative orders to authorise the new standards called for by professional groups. Experts interviewed are concerned that the process could be slow and potentially result in conflicting and incomplete sets of standards. To avoid this, follow-on administrative orders could take a more holistic approach, broadening the conditions for agreed data standards for all the purposes in the public interest (direct care and secondary data uses that would benefit the public, including quality monitoring). Follow-on administrative orders must also ensure that standards are not limited to health care data, but also include public health and social care data which are key to an integrated health information system.

The current approach reduces benefits while increasing risks to data privacy

A fragmented approach to health data management creates (a) missed opportunities to generate improvements in health and other desirable outcomes, and (b) heightened risk of personal health data being compromised. A recent example of a potentially preventable health data privacy breach was due to an absence of stronger security requirements on institutions handling personal health data and resulted in attempts to sell individuals' COVID-19 status on the dark web (see Box 2).

Box 2. COVID-19 data breach could be avoided by stronger governance

In February 2021 there were local and international media reports of a large breach of personal health data from the systems of the Municipal Health Services (GGD). The GGD is responsible for Covid-19 testing and vaccinations. Media reports and experts interviewed by the OECD indicated that there was a lack of safeguards including a lack of staff data access controls, gaps in the tracking of staff data access, inadequate supervision of data protection, inadequate staff training in data protection, and a lack of system-level data protection against the risk of data downloading.

A strong, national data governance framework, with requirements for data custodians to adopt and maintain a privacy-by-design approach to their IT systems and with the controls and safeguards required of data custodians that are set out in the OECD Recommendation on Health Data Governance, may well have limited or avoided the egregious data breach (see Annex C). For example, the OECD Recommendation in article 12 sets out safeguards to be implemented within health data custodians including lines of accountability, data privacy and security training for all staff members, formal risk management processes, and technological, organisational and physical measures designed to protect privacy and data security.

Source: (Loohuis, 2021)

Statistics Netherlands (CBS) is an example of good practice, but its remit is limited

Interviews with experts conducted as part of this review identified Statistics Netherlands (CBS) as a model for the appropriate implementation of GDPR requirements and a privacy-by-design approach to data development, linkage, sharing and accessibility that is secure and privacy-protective. Several health care data custodians indicated that they are sharing their data with Statistics Netherlands and that they benefit from the CBS' secure remote data access facility when their data are shared with external researchers.

Experts from CBS have indicated that they welcome expanding their data holdings of health and health care data and have ambitious plans for providing secure data access within the ODISSEI initiative which includes advanced technical infrastructure and computing power for complex data analysis and software development. Indeed, experts report that CBS is becoming the main provider of secure remote data access services in the Netherlands for both health and social-economic data.

However, CBS experts also report that their authorising legislation makes it difficult for them to receive health datasets from other organisations because they are, by law, required to create national statistics from any dataset they accept. Under these arrangements, CBS cannot become a hub for secure health data linkage and access for research purposes.

Further, CBS is not funded to provide data linkage and access to data. It employs a cost-recovery model that experts interviewed indicate is expensive. The ODISSEI initiative, for example, has funding from universities through scientific grants that help to offset the costs of data access for research.

The approach to electronic health and medical records is un-coordinated

A well designed, longitudinal (interoperable) electronic health record (eHR) system can greatly enhance care quality – especially coordination and integration – as well as supply valuable information for research, innovation and public health.

For example, an individual with multiple health problems can manage their health much better if they have access to their own medical information, and if all their healthcare providers – GPs, specialists, hospitals, emergency rooms, pharmacists, dieticians and physiotherapists – also have access to the same information. This is now eminently possible in countries such as Estonia, Finland and New Zealand.

Moreover, data can be extracted from the eHR system for quality monitoring, clinical registries and health statistics which is common practice among many OECD countries now. The data within the eHR system can be linked to other datasets to, for example, develop machine learning algorithms to predict the mortality risk in sub-strata of patients thereby improving the safety and effectiveness of care in close to real-time. Such risk stratification models are being developed in Israel and Spain.

A longitudinal eHR system does not mean a single, centralised electronic medical record (eMR). It can equally comprise a distributed network of eMRs belonging to hospitals, specialists' rooms, GPs and pharmacies if the technical and operational infrastructure exists for data to be exchanged between them, and where people can access all their own health information in one place.

The lack of eMR interoperability means that patients and the public are missing out on better care and more knowledge to improve care coordination and integration, public health, and research and innovation.

The Netherlands is lagging other countries in eMR interoperability

The situation in the Netherlands is not as advanced as in many other OECD countries regarding interoperability of medical data. While notable initiatives such as MedMij and LSP are trying to address this, the lack of coordination and steering is evident.

Experts interviewed described that most healthcare organisations have engaged software vendors to develop bespoke eHR platforms to specifications that suit their requirements and priorities. In most cases, and in the absence of an overarching national data strategy and governance framework, little attention has been paid to exchanging data. Experts described that many providers are locked into agreements with their vendors, who either limit or charge large sums to retrofit interoperability and exchange capability into their systems.

Stakeholder interviews suggest that patients often need to bring paper records of their health information to different practitioners, and that general practitioners are unable to share important data such as COVID vaccination status with public health officials. Recent media reports describe patients transferred between hospitals needing to carry a CD containing their medical information because the hospitals' eMRs cannot exchange data.[3]

In 2016, the OECD surveyed countries regarding the readiness of their electronic health record systems to contribute to national information and research (Oderkirk, 2016). While the Netherlands did not participate in this survey, progress in other OECD countries could be considered when developing a system in the Netherlands (A follow-up survey is currently under way; the information regarding progress will be included in the final report).

[3] https://eenvandaag.avrotros.nl/item/gegevens-op-de-fax-of-een-dvd-bij-verplaatsing-van-coronapatienten-wordt-gemis-van-elektronisch-patientendossier-wel-heel-duidelijk/

Success is characterised by national coordination and leadership

In 2016, most OECD countries surveyed had: 1. established a **national organisation** that was responsible for setting national clinical terminology and electronic messaging (exchange) standards; 2. specified a **minimum dataset** to be exchanged among authorised users nationally; 3. used **unique identification** of patients and health care providers; and 4. adopted **international terminology standards** for diagnoses, medications, laboratory tests and medical images (Annex B Table 5).

Half of countries:

1. Had exchange of information at the national level, including data sharing among physician offices and hospitals about patients' treatment, medication use, laboratory tests and images;
2. Had a dedicated virtual space (e.g., internet portal) where patients could both access and interact with their own electronic health record; and
3. Were extracting data from the eHR system to populate national health datasets and registries.

Countries reported several levers to improve the spread and interoperability of their electronic clinical data.

- Seven had a legal requirement for health care providers to adopt an electronic health record system (software) that conformed with national standards for both clinical terminology and electronic messaging (exchange).
- Eleven countries had a certification of eHR system (software) vendors that required them to adopt national standards for terminology and electronic messaging.
- Thirteen countries had financial incentives for health care providers to adopt and maintain eHR systems (software).

Collaboration and data exchange are limited

An integrated health information system means that all types of healthcare, public health and social care data can flow to where they are needed and are fit for use upon arrival. In the context of the Dutch health system, this means enabling secure data exchange across the numerous silos and requiring strict technical and semantic interoperability standards.

Timely and secure data exchange opens entirely new possibilities in biomedical science as well as health service design and delivery. For example, the capacity to link various clinical, administrative and social datasets to study the safety and effectiveness of COVID-19 vaccines in various population sub-groups in real time. Results can alert providers and policy makers to potential risks and opportunities, as well as contribute to global efforts to control the pandemic. Such studies have recently been conducted in Israel and Scotland.

In another example, New Zealand has been able to generate 'virtual' registries by harvesting data from a range of sources, saving time and resources.

Despite many stakeholders' best efforts over the past decade, experts interviewed described how strong collaboration and smooth exchange of data are largely lacking in the Netherlands. This can be attributed to several legal and policy barriers discussed in this section.

Rules to protect competition inhibit collaboration and data exchange

The managed competition model is the basis of the Dutch health system. This requires, by definition, a strong regulatory framework. However, some regulations and policies are in direct opposition to promoting data integration. For example, to protect the functioning of the healthcare market, collaboration between providers is monitored by the Netherlands Authority for consumers and markets (acm.nl). Experts

described that, under this authority, collaboration among health care providers generally prohibited except under certain conditions.

The tension between supporting market competition and fostering smooth, secure data exchange and, more broadly, collaboration among providers, needs to be explicitly acknowledged and addressed.

Agreements lack requirements for data interoperability that cannot be overcome by voluntary data exchange initiatives

Experts interviewed explained that multiple institutes are funded by the government to collect data on aspects of health or parts of the healthcare system. However, funding is not contingent upon collaboration among them and data interoperability among them is not required.

Similarly, 'hoofdlijnakkoorden' (outline agreements) between the government and specific sectors such as medical specialists, include agreements on finances and quality but not on data interoperability. As a result, sectors continue to operate in silos.

Experts also explained that standards developed by either Nictiz or MedMij are voluntary and participation in a data exchange is voluntary.

Further, experts described that while the government provides financial incentives to physicians and hospitals to become MedMij certified; certification does not include verification that the data within MedMiJ are interoperable, nor verification that the user experience for patients would meet reasonable expectations. For example, verification of how well health information is integrated and presented to the patient is not included.

Data coverage gaps are evident

Two private data exchanges exist: LSP for exchange among providers and MedMij for exchange between providers and patients. Experts interviewed explained that the LSP is a centralised architecture and the MedMij is developed through open Application Programming Interfaces. A decision is needed to develop a harmonised approach, which would allow for exchange among all stakeholders and avoid unnecessary duplication. Both exchanges are non-binding and therefore they are incomplete, which limits their usefulness for direct care and secondary uses and compromises patient safety.

Experts explained that under current policy, MedMij is conditional upon a patient having a PGO (personal data environment). Patients without a PGO will be missing from MedMij. Also, patients who see providers that are not MedMij certified will be missing part of their health records. For health care providers, MedMij will be an incomplete information source, missing patients and providing incomplete information for patients.

Further, experts also indicated that Personal data environments (PGO) are evolving for sub-sets of patients rather than toward an integrated PGO that provides a complete source of information. The consequence will be that many patients may never have a complete picture of their health and healthcare within a single PGO. This problem will likely be most evident for patients with multi-morbidity or complex health and social care needs.

The health information exchange (LSP) is funded by health insurers. Costs to participate are borne by health care providers and legislation requiring consent (see above) limits its usefulness because some patients are inevitably missing and there are missing data for included patients.

Costs of interoperability are high and exacerbated by information blocking

The Dutch government plans to invest in integrated care through the 'right care at the right place' initiative. Integrated care requires data interoperability among health and social care providers. In addition to legal

barriers to the exchange of data that were discussed earlier, there are resource and technical constraints to health data exchange that will limit reaching the goal of integrated care.

Experts interviewed explained that a large vendor of electronic health record system software in the Netherlands, which provides eHR software to both hospitals and primary care offices, has an IT architecture that limits data exchange and locks health care providers out of accessing their own data.

Experts interviewed indicate that hospitals and medical offices are unable to access their own data and must go through the software vendor to enable data exchange or to enable views of their data (business intelligence tools). This creates a financial disincentive for health care providers to exchange data, as they face financial charges to do so. Further, when financial incentives may be provided by the government to encourage data exchange, the rewards are taken up by the fees of the software provider.

Health care providers experiencing this information blocking are also limited in their ability to adopt new devices, apps and decision-support tools that are set up for a modern IT architecture. At the same time, the Dutch technology sector is limited from creating devices, apps and tools that could be sold in both domestic and international markets.

The situation is likely to continue without legislation, certification and financial incentives to prevent information blocking by software vendors and to encourage software vendors to provide modern IT architectures that support data exchange and analytical uses of data that are in the public interest. This can, in fact, create a level playing field for competition and the market to thrive while advancing public policy objectives.

An updated reimbursement model would create better incentives to collaborate

The current healthcare remuneration model encourages more activity and service volume. In addition to laws explicitly forbidding collaboration (see section 2.4.1), funding based on fee-for-service further disincentivises collaboration and integration of care across sectors and settings because the provider is rewarded simply for their input item in the broader care cycle. Not only can this result in sub-optimal patient experiences and health outcomes, but it is also often more expensive.

Experts interviewed explained that there are calls to change the funding model to encourage coordination and value across entire cycles of care, as opposed to paying for processes and inputs. Bundled payments for an entire care pathway from initial diagnosis to an agreed endpoint can potentially address this problem. Several initiatives using bundled payments have emerged in the Netherlands over the past few years, but this model is not yet the norm.

Because care integration also relies on sharing information about patients and processes, financially rewarding joined-up care and outcomes will de facto also encourage the sharing of information about patients' health and their care. Funding reforms are therefore an integral part of creating an environment where data linkage and exchange makes financial sense. The business case will strengthen if collaboration is rewarded.

Experts interviewed also raised concern about incentives. In the absence of financial incentives for data interoperability, the benefits of data interoperability and integration mainly accrue to government, researchers and health insurers; while the costs of improving the interoperability of health information systems are mainly borne by health care providers. Government leadership and legislative and policy tools are needed to create the right environment for information exchange and collaboration.

The Netherlands risks being left behind on research and innovation

Many countries are gearing up to use data, including health data, as the fuel to power research and innovation. The Netherlands risks being left behind in this regard unless current deficiencies in data governance, interoperability and exchange are addressed.

There are worrying signs. As a result of the various issues with data access and interoperability outlined in the previous sections, interview subjects reported that researchers and AI developers in the Netherlands are frequently working with patient clinical data from other countries, such as the USA and China.

Data as a public good: EU Health Data Spaces

European discussions are underway through the EU Digital Health Strategy toward the creation of an EU Health Data Space (EC, 2021). A new regulation is proposed to support Data Spaces in key economic sectors to create a single market for data, where data from public bodies, businesses and citizens can be used safely and fairly for the common good. In particular, an EU Health Data Space is proposed to "promote better exchange and access to different types of health data (electronic health records, genomics data, data from patient registries etc.), not only to support healthcare delivery (so-called primary use of data) but also for health research and health policy making purposes (so-called secondary use of data)" (EC, 2021a).

Three pillars are proposed to support the Health Data Space:

1. Developing a health data governance framework for EU member states that provides guidance toward secure and privacy protective primary and secondary uses of health data that foster the accessibility and sharing of data. Such guidance would support greater harmonisation of the implementation of EU GDPR requirements in practice.
2. Data quality and interoperability including technical and semantic (terminology) interoperability between the different infrastructures and IT systems and ensuring health data in Europe are FAIR (Findable, Accessibly, Interoperable and Re-Usable).
3. Technical infrastructure that builds upon and scales up EU infrastructure, including the eHealth Digital Service Infrastructure, the European Reference Networks and the Genomics Project.

The technical and semantic interoperability standards for the Health Data Space are expected to include international standards for data exchange and terminology and favour exchange standards that support protection of health data privacy and security. For example, a 2021 policy report of the Standing Committee of European Doctors which represents medical associations across Europe, calls for the Health Data Spaces to adopt the HL7 FHIR standard for data exchange and the SNOMED CT clinical terminology standard (CPME, 2021 Forthcoming).

As the Netherlands evaluates the next steps toward an integrated health information system, emerging EU requirements for a Health Data Space should be seen as an opportunity to provide secure access to health data for monitoring and research. For example, new national bodies have been launched in France and Finland that have characteristics and functions like those envisaged for the Health Data Space. France introduced the Health Data Hub in 2019 and Finland launched FinData in 2020 to provide a unique entry point for secure and privacy-protective data linkage services and access to health microdata that are EU GDPR compliant (see Box 3).

Two Dutch initiatives have features of health data spaces

While there are many health data custodians in the Netherlands, two research infrastructures have emerged whose aims and purpose align with those envisaged for Health Data Spaces.

Hospitals in the Netherlands have provided start-up funding to create the Health Research Infrastructure initiative (Health-RI) which aims to "establish an interconnected data infrastructure for Dutch personalised medicine and health research" (Dutch Tech Centre for Life Sciences, 2021). Experts interviewed indicate that Health-RI would like to access data within hospital and GP electronic health record systems for approved research projects in real time.

Health-RI intends to use the personal health train concept to protect privacy and data security. With the personal health train, analytics and other software code (research questions) travel to where data is held and only research results (answers) flow back to the researcher. This Netherlands innovation is a new privacy-enhancing technology that advances 'privacy-by-design' (see Box 1). Health-RI is seeking permanent funding from the government.

Box 3. Health Data Hub and Findata

The Health Data Hub is part of a national digital strategy and is developed according to a strategic roadmap. It was created to support France in becoming a leader in Artificial Intelligence in health and to overcome barriers to the re-use of health data for research. The Hub is a public interest group that was authorised by law and funded by the government to expand upon the existing national health data system (SNDS) to encompass all existing databases concerning publicly funded health activities (e.g. hospital electronic health records warehouses, cohorts, and registries). Members of the Hub include public authorities, health insurance funds, research institutes, health professionals and the life science industry. A mission of the Hub is to elaborate a Citizens and Patients Charter in collaboration with patients' associations. An independent ethical committee reviews requests for access to data and the final approval decision is taken by CNIL which is the authority responsible for the protection of personal data in France. The Hub is transparent to the public regarding the procedure for access to data, data protection and the projects that are approved.

FinData is authorised by law to support secondary uses of health and social data in Finland for projects that contribute to the public interest. Findata is the only authority that can issue permits for the secondary use of health and social data when the data is compiled from more than one data custodian. Findata provides for the secure linkage and research access to publicly funded datasets and registries including the data holdings of the Finnish Institute for Health and Welfare (THL), the Social Insurance Institution of Finland (Kela), the Population Register Centre, the Finnish Centre for Pensions and Statistics Finland. From 2021, Findata will expand to include data within the national EHR system (Kanta). A steering group guides FinData's operations and includes representatives appointed from the Ministry of Social Affairs and Health, the Finnish Institute for Health and Welfare, the Social Insurance Institution of Finland, the Finnish Centre for Pensions, the Digital and Population Data Services Agency, Statistics Finland, the Finnish Institute of Occupational Health, the Finnish Medicines Agency, and representatives of social welfare and health care service providers. Operations are supervised by Ombudsmen for the parliament and for data protection.

Sources: Stuwe, 2020; FinData, 2021; Oderkirk, Survey Results: National Health Data Infrastructure and Governance, 2021

A second research infrastructure is ODISSEI (Open Data Infrastructure for Social Science and Economic Innovations) provides researchers with access to the data holdings of the CBS, including the micro-data in-flowing to CBS from Dutch Hospitals, GPs, health insurers and research institutes as well as health survey data and information on the health care industry (ODISSEI, 2021).

Experts interviewed explained that ODISSEI follows 'privacy-by-design' practices to offer secure data linkage services and secure access to data, as well as an advanced computing and analytic capacity. Funding for ODISSEI is through scientific grants that subsidise the costs of data linkages, infrastructure and secure access to data enabling CBS to provide services to ODISSEI members at a lower cost.

ODISSEI's membership includes social data research centres and, more recently, medical research centres have joined as observers. Experts interviewed explained that medical research centres are attracted to the model ODISSEI provides, where ODISSEI sets the research strategy and the CBS provides data curation, linkage and secure remote data access. Further, there is interest in the research community to bring the social sciences and the life sciences closer together because of their overlapping research objectives and data needs.

Health research projects, particularly those in the public health domain where the influences of environment, health behaviours and socio-economic factors are important, take place within ODISSEI. For example, recent projects include a study examining genome-wide associations with health care costs and an analysis of how behaviours and inequalities spread through social networks. There are, however, important research centres and health data that are outside of ODISSEI. Experts interviewed explained, for example, that it has not been possible to link the social networking model developed within ODISSEI to the COVID-19 case data collected within RIVM. If such exchanges were more feasible, then it would be possible to leverage the investment in the social networking model to predict how and where the pandemic may be spreading, and which population groups are at highest risk. This information could guide public policy decisions.

ODISSEI reports a shortfall in governmental funding for national cohort surveys that follow individuals over a long period of time. Longitudinal data from cohorts provides unique information about how the trajectory of individuals' health, behaviours and environments influence their future health outcomes and health care use. Such data is not available from clinical or administrative data sources.

As the strategy for an integrated health information system is developed, it will be important to consider how the Health RI project and the ODISSEI project can be connected with one another and with all the key data that are needed for the Netherlands to reach its public policy goals.

Toward an integrated health information system in the Netherlands

OECD health systems taking advantage of digital technology and data are all organised and funded differently. But they share a common objective: they are developing an integrated health information system based on a national health data governance framework and the strategies, roadmaps, organisations, funding, and leadership necessary to ensure adherence.

A health data governance framework is an indispensable part of a modern, 21st century health system that seeks to embrace the opportunities of health data in a way that protects individuals' rights to privacy. It comprises legislation, policy and regulation on standardisation, interoperability, and exchange; on security and privacy requirements; and on public transparency and engagement to ensure necessary levels of trust among the public and other key stakeholders.

A cohesive, national framework is necessary in any context, but especially in countries with a fragmented health data ecosystem such as the Netherlands. The alternative -- a collection of data silos that cannot and/or will not exchange valuable information, and where management of data security and privacy risks is ad hoc and very variable -- is not in the interest of patients, providers, industry, governments, or the public, and will hinder the realization of the four policy goals outlined in the introduction.

This section sets out the requirements to address the problems; to take advantage of strengths described in the previous section; and to develop an integrated health information system. The first requirement is a mindset that sees data as a public good and a resource that can be harnessed to advance public and commercial interests. This needs to be embodied in a National Strategy that must be developed inclusively and be trusted by all stakeholders. A range of policies, regulations and enabling legislation will be needed to implement the national strategy. Finally, technical infrastructure and standards will also need to be developed.

Data as a public good

Countries making strides in putting their data to work have recognised that data are a valuable resource that should be used to generate public benefits. Significant public investment in health and health care are a key reason why health data are a public good – this includes public investment in health care provision, in health data development and in funding health research.

But there is also an economic argument for seeing data as a public good in the modern era of 'Big Data', ;high performance computing and modern analytical techniques including machine learning and artificial intelligence. Data represent immense value both because of the information they potentially contain and because they can be used and re-used ad infinitum. Their use by one actor does not preclude their use by others.

More importantly, like other public goods such laws or language, data are instrumental in building social value through knowledge and information. Their exclusivity is not intrinsic, but is imposed by man-made laws, conventions, and institutions. In net terms, their commodification hampers human development.

Moreover, the social and economic value of data increase exponentially with their size. For example, a researcher looking for biomarkers that will uncover a precision therapy will find a single dataset comprising 10 million records is much more valuable than 100 separate datasets of 100,000 patients that cannot be linked or analysed as a whole (such as via the personal data train).

In the modern data ecosystem, a company will stand to profit by accepting that even a small slice of analytics on a huge data pool – which cannot be depleted – will generate far greater profits than hoarding much smaller puddles of data for proprietary use.

A national strategy for an integrated health information system

A strategic plan is a common first step toward an integrated health information system. Developing a strategy should consider the data assets and information infrastructure already in place and build forward from them to develop the tracks and signals that are missing. Key to the development of the strategy will be working with stakeholders to determine the objectives the strategy and the values that the stakeholders want to uphold.

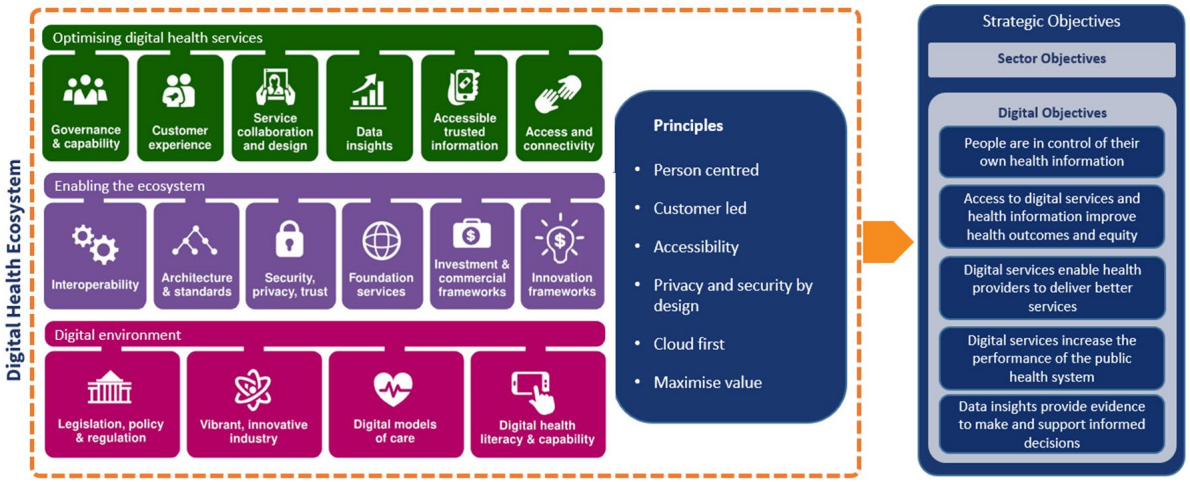
It is essential that the strategy is sufficiently **broad and deep**. Breadth refers to incorporating the three main data types: healthcare, public health, and social care data. Depth ensures that all data are included, and that they can be linked at individual level to enable better care integration as well as more precision and scope in secondary uses.

An important accompaniment to the digital strategy are road maps for each strategic objective, particularly those that will be challenging to achieve, such as data interoperability. The road maps should be specific about who is responsible for what and when deliverables can be expected.

Figure 2 presents a graphical overview of the recently published national digital strategy of New Zealand, which includes many goal posts that would resonate in the Netherlands such as: digital services and health information contribute to patient empowerment; health care quality and outcomes are improved; health system performance is strengthened; and there is greater capacity for evidence-based decision-making.

Essential elements include those that enable the strategy to be realised at a policy level, such as legal reforms, policy guidelines, governing and operational bodies, and financial incentives; as well as those that enable the strategy at a technical level, such as data architecture, technical infrastructure and terminology and interoperability standards.

Figure 2. New Zealand Digital Health Strategic Framework



Source: New Zealand, 2020

National strategy will require leadership and expertise

The Ministry of Health, Welfare and Sport would take the lead in the development of the national strategy. Indeed, all experts interviewed for this country review called for leadership from the Ministry to build the tracks and the signals. The Ministry must be supported in developing the strategy by experts, particularly external experts in health data informatics, data interoperability and health data science, as well as external experts in 'privacy-by-design' approaches to health data governance.

Internal support will also be needed for the Ministry to build a team to take the lead. The ministry could consider creating a new unit and engaging or seconding experts in health information systems, health data science and informatics and health data governance. This expertise will be essential to ensuring an effective national strategy.

The Information Council can become a formal advisory body

A potential advisory body for developing and implementing the national strategy is already in place, the Information Council (IC). As previously mentioned, the IC currently lacks participation from key organisations with responsibility for national health information, including national health care quality registries; national health research infrastructures; and organisations providing national health data access, linkage, and governance.

Ensuring the IC includes representatives from key stakeholders in all aspects of an integrated health information system is highly recommended to make the most informed decisions about the strategy.

Building trust in the strategy

The national strategy will steer the Netherlands away from the current situation of data silos toward an integrated system where secure data exchange is the norm. The strategy should modernise data development, exchange, management, and governance and it will require a change management approach that builds trust.

The Dutch approach of consensus-building and consultation will help. The key will be to allocate sufficient time and resources toward consultation with stakeholder bodies and the public at all points in the

development of the strategy, so that progress from a draft strategy to a final strategy to roadmaps and implementation will feel natural, expected and safe.

Another key will be to have the right input in terms of technical, IT, policy, and legal expertise to develop a worthwhile and trustworthy strategy. Stakeholders will then be more at ease and comfortable to share their needs, their constraints, and their hopes for the strategy.

Members of the advisory body to the strategy, as well as the core strategy team, will be ambassadors and spokespersons for the strategy and should be encouraged to discuss the strategy widely with their communities and with the media to reach the public. For example, we understand from experts we interviewed that having leading Dutch experts speak to the media about the trustworthiness of the Covid-19 monitoring app alleviated the public's concerns about data privacy.

The process of developing the strategy and roadmaps will result in a more complete and well-considered plan than can be developed through this OECD country review. However, the following sections provide insights and sound the alarm on areas that need deeper consideration as the national strategy is developed.

Implementing the national strategy

Implementing the National Strategy and operationalising its various facets can be described as 'building the tracks' of the integrated health information system. It will principally concern developing and maintaining consistent national data standards, and then certifying and incentivising actors to implement the strategy, including healthcare providers, software vendors and other developers of IT solutions.

A national agency tasked with implementation

A single authority will be needed to implement the national strategy. This could be done by 'strengthening' an existing organisation or creating a new agency. In either case, this agency will have the authority to develop consistent national standards for semantics (terminology), electronic messaging (exchange), and data accessibility/sharing. It would also be responsible for keeping the standards up to date.

The agency would best operate under a formal shared governance of standard setting with the existing health research infrastructure organisations and health information organisations (such as Health RI, CBS, ZiN, and ODDISEI), so that the standards developed will cover all data and data uses that are planned for within the National Strategy. It would have formal links with the IC (as the strategic advisory body) and involve the IC in standards development and maintenance.

Certifying and verifying compliance with standards

The agency would be responsible certifying vendors of IT solutions and digital tools for compliance with national standards. It would also certify and verify health care providers and other information system actors have achieved interoperability standards and are exchanging useable data and not blocking data.

This process must go beyond simply demonstrating that standards are used. Proof of data exchange should also be required to achieve certification.

Governance and policy reforms

Key governance and policy reforms constitute 'the signals' that enable data to flow along the newly built tracks. These reforms will be executed by the Ministry, with advice of the IC and will primarily comprise developing new legislation, guidelines, governance, and funding mechanisms.

A firm hand will be needed to address resistance

From the outset it must be foreshadowed that an integrated health information system -- as envisaged here -- will be opposed and resisted by stakeholders who benefit from the current arrangements. For example, a firm hand will be needed with eHR system software vendors whose business model and products are out of alignment with global standards for clinical terminology and data exchange, and who do not support data interoperability within or across health care organisations.

These stakeholders may pressure the government to favour their local IT solutions, but unless compliant with international terminologies and electronic messaging standards, these solutions will not help the Dutch health technology sector to compete globally; will not allow local health care providers to adopt solutions/tools from the global marketplace; and will make progress toward the national strategy expensive, slow and probably impossible.

A legislative framework

Legal authority will be needed to authorise and finance the National Strategy and its implementation. This can be follow-on administrative orders to the new framework legislation for data exchange via care quality standards. They will complement the framework legislation and ensure depth and breadth (i.e. incorporate public health data and social care data and facilitate use of data for secondary purposes). The new administrative orders should require compliance with standards that ensure data interoperability and prevent data blocking by data custodians and software vendors.

Revisions may be needed to legacy legislations that are posing unnecessary obstacles to an integrated health information system, such as revisions to the *Medical Treatment Contracts Act (Wgbo)* to allow for lawful alternatives to consent for data exchange and uses in the public interest; to legislation authorising the Central Bureau of Statistics to allow it to act as a central hub for access to health datasets; and to regulations related to consumers and markets that prevent health care collaborations and data integration.

Regulation and guidelines

National policies will be needed to fulfil regulatory requirements that enable access to data for those who need them, while also keeping data secure and maintaining individuals' rights to privacy. These will guide:

- Implementing the GDPR by all actors in the health information system
- Emphasising privacy-by-design
- Adhering to FAIR principles, and
- Developing reasonable approaches or lawful alternatives to consent.

It is critical that these national policies align with existing and developing guidance and regulations at the European level.

As part of this reform, the functionality and capacity of the two data exchanges (LSP and MedMij) should be harmonised to meet the needs of all stakeholders, including those currently using MedMij and LSP, and to realise the goals of the national strategy. The exchange of data should ensure full coverage of patients and providers and that patient records are complete. The exchange should be legally authorised, follow a 'privacy-by-design' approach and meet international standards for data security.

Complementary funding and incentives

To complement laws and policies, financial incentives will be needed to encourage compliance with national GDPR guidelines, with national data standards, and for demonstrating (verifiable) data interoperability.

This will require a review of government funding and subsidies of activities related to the exchange and use of health data, including research projects funded by government grants. It may also require explicit financial incentives to encourage health care providers and other actors to move to certified IT solutions and succeed in achieving verifiable interoperability.

The Ministry and IC should consider how broader reforms to healthcare funding and remuneration that reward care coordination and value will affect the functioning of an integrated health information system.

Technical infrastructure and standards

The policy and regulatory infrastructure required to create an integrated health information system was outlined in the preceding sub-sections. However, several technical requirements will also require attention, particularly if the system is to be retrofitted on top of the existing arrangements.

To facilitate information development and analytics, it will be necessary in many cases to re-code existing data to a common a data model. Leading global health data models should be selected for this purpose and the technical capacity instituted.

Similarly, modern IT architecture and global or European standards for data terminology and exchange (messaging) should be deployed. For the Netherlands to participate in multi-country research and monitoring, the standards must comply with current and emerging European regulations. It will also be an advantage if the Netherlands participates in global and European efforts to develop global standards for health data terminology and exchange.

These functions can be performed by the agency responsible for operationalising the national strategy, in close liaison with the IC and Ministry. However, the need for expertise in IT architecture is again emphasised.

References

Cavoukian A (2006, November), Privacy By Design: The Seven Foundational Principles. Retrieved April 8, 2021, from IAPP Resource Centre: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

CPME (2021 Forthcoming), CPME Policy on the European Health Data Space. Belgium.

Dutch Tech Centre for Life Sciences (2021), Health-RI. Retrieved from https://www.dtls.nl/large-scale-research-infrastructures/health-ri/

EC (2021), European Health Data Space. Retrieved 04 01, 2021, from https://ec.europa.eu/health/ehealth/dataspace_en

EC (2021a), e-Health Digital Health and Care - European Health Data Space. Brussels. Retrieved from https://ec.europa.eu/health/ehealth/dataspace_en

EDPS (2020), Preliminary Opinion 8/2020 on the European Health Data Space. European Data Protection Supervisor. Retrieved from https://edps.europa.eu/sites/default/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf

FinData (2021), Retrieved April 8, 2021, from FinData: Health and Social Data Permit Authority: https://www.findata.fi/en/

Hashiguchi TCO, Slawomiriski L and Oderkirk J (Forthcoming), Laying the Foundations for Artificial Intelligence in Health. Paris: OECD Publishing.

Health RI (2021), Personal Health Train. Retrieved from https://www.health-ri.nl/initiatives/personal-health-train

Loohuis K (2021, February 8), Data of thousands of Dutch citizens leaked from government Covid-19 systems. Computer Weekly.

New Zealand (2020), Digital Health Strategic Framework. Retrieved from https://www.health.govt.nz/our-work/digital-health/digital-health-strategic-framework

Oderkirk J (2016), Readiness of Electronic Health Record Systems to Contribute to National Health Information and Research. Paris: OECD Publishing. https://dx.doi.org/10.1787/9e296bf3-en

Oderkirk, J (2021), Survey Results: National Health Data Infrastructure and Governance. Paris: OECD Publishing. https://dx.doi.org/10.1787/9789264244566-en

ODISSEI (2021), Retrieved from https://odissei-data.nl/en/

OECD (2019), Recommendation of the Council on Health Data Governance. Paris: OECD Legal Instruments. Retrieved from https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf

OECD (2020), Opportunities and Challenges of Blockchain Technologies in Health Care. Policy Breif

OECD Blockchain Policy Series. Retrieved from https://www.oecd.org/finance/blockchain/Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf

Stuwe L (2020, June), Health Data Hub: Overview, Strategy and Lessons Learned. Retrieved April 8, 2021, from eHAction: http://ehaction.eu/wp-content/uploads/2020/10/D3S2_HDH-Louisa_Stuwe-new_version.pdf

Annex A: Consultation with experts

The recommendations presented in this report were supported by a series of interviews and focus group discussions conducted by the OECD team with experts in the Netherlands from February to April 2021. Initial interview subjects were identified by the Ministry of Health and Welfare. These interview subjects recommended other experts for the OECD to consult. The OECD continued interviews until the information gathered from key informants began to share similar messages. Further rounds of interviews and focus groups are planned to take place in the coming months. These discussions will aim to refine the recommendations presented in this document.

The OECD thanks and appreciates the contributions of the following experts whose insights, experiences and aspirations informed the development of these recommendations.

Table 1. Experts interviewed about the health information system in the Netherlands

Name	Position	Organisation
Caroline A. Baan	Science Officer	Ministry of Health, Welfare and Sport
Frank Berens	Policy Advisor	V&VN (Organisation of nurses)
Adriaan Blankenstein	Chief Executive Officer	VZVZ (Association of care providers for care communication)
Teresa Cardosa	Senior Policy Advisor	ZiN National Care Institute
Herko Coomans	Digital Health Policy Coordinator	Ministry of Health, Welfare and Sport
Dirk Deelstra	Senior Policy Advisor	ZiN National Care Institute
Tom Emery	Deputy Director	Open Data Infrastructure for Social Science and Economic Innovations (ODISSEI)
Leone Flikweert	Chief Executive Officer	Health Research Infrastructure (Health RI)
Jeroen Geelhoed	Senior Manager	BeBright Consulting
Ronald Gijsen	Researcher	National Institute for Public Health and the Environment (RIVM)
Ivo LWJ Gorissen	Account Manager	Central Bureau of Statistics (CBS)
Jan Hazelzet	Professor in Healthcare Quality and Outcomes	Erasmus University Medical Centre
Marcel Heldoorn	Manager, Digital Healthcare	Netherlands Patient Federation
Peter Jansen	Information Manager	ZN (Organisation of health insurers)
Anil Jadoenathmisier	Director, IT and Innovation	VZVZ (Association of care providers for care communication)
Sander Klous	Partner, Big Data Analytics	KPMG
Frits van Merode	Professor of Logistics and Operations Management in Healthcare	Maastricht University Medical Centre Maastricht University
Lokke Moerel	Professor of Global ICT Law	Tilburg University
Isabel Moll	Partner, Digital Trust Data (Healthcare)	KPMG
Annemiek Mulder	Senior Policy Advisor	ACTIZ (Organsation of LTC/home care providers)
Yola Park	Adviser, Information Policy	Ministry of Health, Welfare and Sport
Ron Rozendaal	Director, Information Policy and CIO	Ministry of Health, Welfare and Sport
Charlotte de Schepper	Representative	KNOV (Organisation of midwives)
Gert-Jan van Boven	Chief Executive Officer	Dutch Hospital Data
Lies van Gennip	Director	Stichting PALGA (Pathology Registry)
J.A.M. van Oers (Hans)	Professor of Public Health	Tilburg University
Vincent Van Polanen Petel	Head, Health and Social Care Statistics	Central Bureau of Statistics (CBS)
Maarten van Rixtel	Chief Executive Officer	Sensor (Organisation of LTC/home care providers)
Inez Young	Chief Data Officer	National Institute for Public Health and the Environment (RIVM)

Annex B: Tables

Table 2. Custodians of Netherlands key national health datasets

Key National Health Dataset	Dataset Custodian
Hospital in-patient data	Dutch Hospital Data (DHD) + Statistics Netherlands (CBS)
Mental hospital In-patient data	NZa (National Health Care Authority)
Emergency health care data	Veiligheid NL (Consumer and Safety Institute)
Primary care data	Nivel (Netherlands Institute for Health Services Research)
Prescription medicines data	Zorginstituut Nederland (National Health Care Institute)
Cancer registry data	Netherlands Comprehensive Cancer Organisation (IKNL)
Diabetes registry data	DPARD (Dutch Pediatric and Adult Registry of Diabetes)
Cardio-vascular disease registry	Nederlande Hart Registratie (Dutch Heart Registration)
Mortality Data	Statistics Netherlands (Centraal Bureau voor de Statistiek)
Formal long-term care data	Several organisations (CIZ, Het CAK, NZa, ZIN, SVB, Bureau Jeugdzorg, Vektis)
Patient experiences survey data	n.a.
Population health survey data	Statistics Netherlands (Centraal Bureau voor de Statistiek)
Population Census/Registry data	Statistics Netherlands (Centraal Bureau voor de Statistiek)

Source: OECD 2019-20 Survey of Health Data Development, Use and Governance. See Oderkirk, J (2021).

Table 3. Sharing and access to de-identified data varies by health dataset custodian

Analysts from the following organisations could be approved access to de-identified data for statistical or research purposes in the public interest

	Hospital in-patient data	Mental hospital in-patient data	Emergency health care data	Primary care data	Prescription medicines data	Cancer registry data	Diabetes registry data	Cardio-vascular disease registry data	Mortality data	Formal long-term care data	% of national health care datasets
Government ministry or government national data custodian	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	80%
University or non-profit research institute	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	80%
Health Care Provider	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	70%
For-profit business	No	No	No	No	Yes	No	No	Yes	No	No	20%
Foreign university or non-profit research institute	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	60%

Source: Source: OECD 2019-20 Survey of Health Data Development, Use and Governance. See Oderkirk, J (2021).

Table 4. Data protection and security policies and practices vary by dataset custodian

	Hospital in-patient data	Mental hospital in-patient data	Emergency health care data	Primary care data	Prescription medicines data	Cancer registry data	Diabetes registry data	Cardio-vascular disease registry data	Mortality data	Formal long-term care data	% of national health care datasets
Legislation authorises dataset creation	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes2	80%
Data Protection officer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes2	Yes	100%
Control and tracking of staff data access	Yes	Yes	No	No	No	Yes	Yes	No	Yes	Yes	60%
Process to assess risk of data re-identification	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	70%
Treatment of variables posing a reidentification risk	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	80%
Public description of the dataset including its legal basis	Yes	No	Yes	Yes	Yes	n.r.	Yes	Yes	Yes	No	70%
Sharing data with external researchers is legally authorised	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes	Yes	70%
Individuals consent or opt-out to data sharing	No	Opt-out	Opt-out	Opt-out	Consent	No	Opt-out	No	Consent/ opt-out	Consent	70%
Procedure to request access to data and approval criteria are public	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	80%
Procedure to request a dataset linkage and approval criteria are public	n.a.	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	60%
Approval body for dataset linkages	n.a.	n.r.	Veiligheid NL (Consumer and Safety Institute)	GPs and privacy committee	n.r.	n.a.	n.a.	Board of directors	Central Bureau of Statistics	Health care insurers	50%
Standard data sharing agreement	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100%
Secure remote	Yes	Yes	No	No	No	No	No	Yes	Yes	No	40%

data access service											
Supervised research data centre	No	No	No	No	No	No	No	Yes	Yes	Yes	30%

Source: OECD 2019-20 Survey of Health Data Development, Use and Governance. See Oderkirk, J (2021).

Table 5. National electronic health record system development in OECD countries in 2016

Country	National system includes information sharing among physicians and hospitals about treatment, medication, lab tests and images	Minimum dataset has been defined	Unique patient and provider identifier	National organisation responsible for clinical terminology and electronic messaging standards	Legal requirement to adopt eHR systems that conform to clinical terminology and electronic messaging standards	Certification requires vendors to adopt national standards	Financial incentives to adopt and maintain high quality eHR systems	Patients can view their own eHRs (patient portal)	National health datasets created from eHRs
Australia	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
Austria	Yes	No	Yes	Yes	Yes	n.r.	Yes	Yes	No
Canada	Yes	Yes	Yes	Yes	No	n.r.	Yes	Yes	Yes
Chile	No	No	No	Yes	No	Yes	Yes	No	No
Croatia	No	Yes	Yes	Yes	Partial	Yes	No	No	No
Czech Republic	No	Yes	Partial	Partial	No	n.r.	No	No	No
Denmark	Yes	Yes	Yes	Yes	Yes	n.r.	No	Yes	Yes
Estonia	Partial	Yes	Yes	Yes	Yes	n.r.	Yes	Yes	No
Finland	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
France	Yes	Yes	Yes	No	Partial	Yes	No	Yes	No
Greece	Partial	Yes	Yes	No	n.r.	n.r.	No	Yes	Yes
Iceland	Partial	Yes	Yes	Yes	No	n.r.	No	Yes	Yes
Ireland	No	Yes	Partial	No	Partial	No	No	No	Yes
Israel	Yes	Yes	Yes	Yes	No	n.r.	Yes	No	Yes
Japan	No	Yes	No	Yes	No	n.r.	No	No	n.r.
Latvia	Partial	Yes	Yes	Partial	No	n.r.	No	Yes	No
Luxembourg	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Mexico	No	No	Yes	No	No	Yes	No	Yes	Yes
New Zealand	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
Norway	Partial	Yes	Yes	No	n.r.	No	Yes	Yes	Yes
Poland	Yes	Yes	Yes	Yes	Yes	n.r.	No	No	Yes
Singapore	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Slovakia	Partial	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Spain	Yes	Yes	Partial	Yes	No	n.r.	Yes	Yes	Yes
Sweden	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
Switzerland	Yes	Yes	Yes	Yes	No	n.r.	No	Yes	No
UK England	Partial	Yes	Yes	Yes	No	Yes	Yes	Yes	No
UK Northern Ireland	Yes	No	Yes	No	No	No	No	No	No
UK Scotland	Partial	Yes	Partial	Yes	No	Yes	Yes	Yes	Yes
United States	No	Yes	Partial	Yes	No	Yes	Yes	Yes	Yes

Note: The Netherlands did not participate in this survey.
Source: 2016 OECD Survey of Electronic Health Record System Development and Use. See Oderkirk 2016.

Annex C: OECD Recommendation on Health Data Governance

The OECD Council Recommendation on Health Data Governance recommends that governments establish and implement a national health data governance framework to encourage the availability and use of personal health data to serve the health-related public interest while promoting the protection of privacy, personal health data and data security (OECD, 2019). The Recommendation sets out 12 key principles that health data governance frameworks should provide for. They are summarised as follows:

1. Engagement and participation, notably through public consultation, of a wide range of stakeholders to ensure the framework serves the public interest and is consistent with societal values.
2. Government coordination and promotion of cooperation among organisations processing personal health data, whether in the public or private sectors, to encourage common data terminology and interoperability standards and common procedures to minimise barriers to sharing data for uses in the public interest.
3. Review of the capacity of the public sector to process personal health data for research, statistical and other uses within the public interest - including data availability, quality, accessibility and privacy protection.
4. Clear provision of information to individuals about the processing of their personal health data and timely notification of a data breach.
5. Processing of personal health data by informed consent or a lawful alternative. When processing is not based on consent, individuals should be able to object to the processing (opt-out). If opt-out is not possible then individuals should be provided with the reason why and the legal authorisation for the processing.
6. Review and approval procedures for the uses of personal health data that assess if the uses are within the public interest. Reviews should be objective, fair, timely, and transparent to the public.
7. Provide public information about the purpose of processing of personal health data, the public interest served, the procedure and criteria to approve data processing and a summary of approval decisions taken.
8. Maximise the potential of new technologies to support data use and re-use, protect data privacy and security and support individuals' control of the uses of their own data.
9. Monitor and evaluate whether the uses of personal health data have served the public interest and brought the benefits that were expected.
10. Provide training and skills development in privacy and security measures to those processing personal health data.
11. Implement controls and safeguards to:
    a. Provide accountability for personal health data processing, accompanied with mechanisms for audit.
    b. Establish requirements that personal health data can only be processed by organisations with appropriate data privacy and security training for staff members.

c. Organisations processingmais personal health data should designate an employee to be accountable for the organisation's information security programme (Data Protection Officer).
d. Formal risk assessment processes that include the risk of unauthorised data linkages and breaches.
e. Technical, physical and organisational measures to protect privacy and data security.
    i. Mechanisms that limit the identification of individuals while allowing data re-use (linkage).
    ii. Data sharing agreements that specify data security requirements and sanction non-compliance.
    iii. Alternatives to data transfers, such as secure data access centres and remote data access.
    iv. Identity verification and authentication of individuals accessing personal health data.

12. Require organisations processing personal health data to demonstrate that they meet national expectations for health data governance. This can include certification or accreditation.

Source: OECD (2019), Recommendation of the Council on Health Data Governance. Paris: OECD Legal Instruments. Retrieved from https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf

TOWARD AN INTEGRATED HEALTH INFORMATION SYSTEM IN THE NETHERLANDS

DRAFT INTERIM BRIEF AND RECOMMENDATIONS

OECD