

4

Towards an integrated health information system in the Netherlands

This chapter describes the legal, policy and operational changes that are needed in the Netherlands to establish an integrated health information system. It sets out the requirements to take advantage of the strengths and to address the problems uncovered in this review of the current Dutch health information system. The recommendations include an overarching requirement to approach health data more as a public good than as a commodity, and to develop and implement a national digital health strategy that strengthens mutual trust across all stakeholder groups. A range of policy actions to implement the national digital health strategy are recommended in this chapter, including the need for technical infrastructure and interoperability standards, and an overarching data governance framework that includes greater harmonisation of policies and practices to ensure privacy and promote data security.

Many OECD countries have started harnessing their health data to work to achieve their public policy objectives. Although the health systems are all organised and funded differently, they share some common features: an integrated health information system based on a co-ordinated strategy that is supported by strong leadership and a specifically designed data governance framework.

The preceding two chapters described how personal health data, as well as other data relevant to health and well-being, are managed, exchanged, and deployed to advance policy objectives in the Netherlands including service improvement, better public health, research outputs and innovation. Despite some considerable strengths and advantages, the current health information landscape is too fragmented to achieve these goals and presents a risk to the Netherlands of falling behind other countries in a range of social and economic domains.

This chapter outlines legal, policy and operational changes to establish an integrated health information system. It sets out the requirements to take advantage of strengths described in the previous chapter and to address the problems uncovered in this study.

The first requirement is a mindset that sees data as a public good and a resource that can be harnessed to advance the health and welfare of the Dutch people. 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. Technical infrastructure and standards will need to be implemented. An overarching governance framework will be required, including greater harmonisation of data privacy and security policies and practices.

Steps toward an integrated HIS

The foundation of a modern, 21st century health information system that seeks to embrace the opportunities of health data while protecting individuals' rights to privacy is a modern, robust data governance framework. Such a framework 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. In effect, it is a technical, policy and political apparatus.

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 realisation of the four policy goals outlined in the introduction.

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 the increasing quantity of generated health data calls for a political choice, legislative guidance and fitting strategic action in order to facilitate ethical and optimal use of this rapidly expanding commodity. The challenge does not lie within specific actors in the health system, but across all of them. There is a need to have a common infrastructure in order to have health data that is fit for use and purpose for each actor's mandate in the health system because, fundamentally, most health system actors are reliant on data generated by others to achieve their objectives.

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 a unified national strategy (preferably aligned with a broader national digital/data strategy). It will require a new set of institutional function to develop, implement and oversee a health data infrastructure and integrated information system, either through a

new national authority or by consolidating and strengthening the remit, function, and competencies of existing agencies. Successful implementation will require good governance, policy, and trust among all stakeholders.

A unified, national strategy is needed

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 of the strategy and the values that the stakeholders want to uphold.

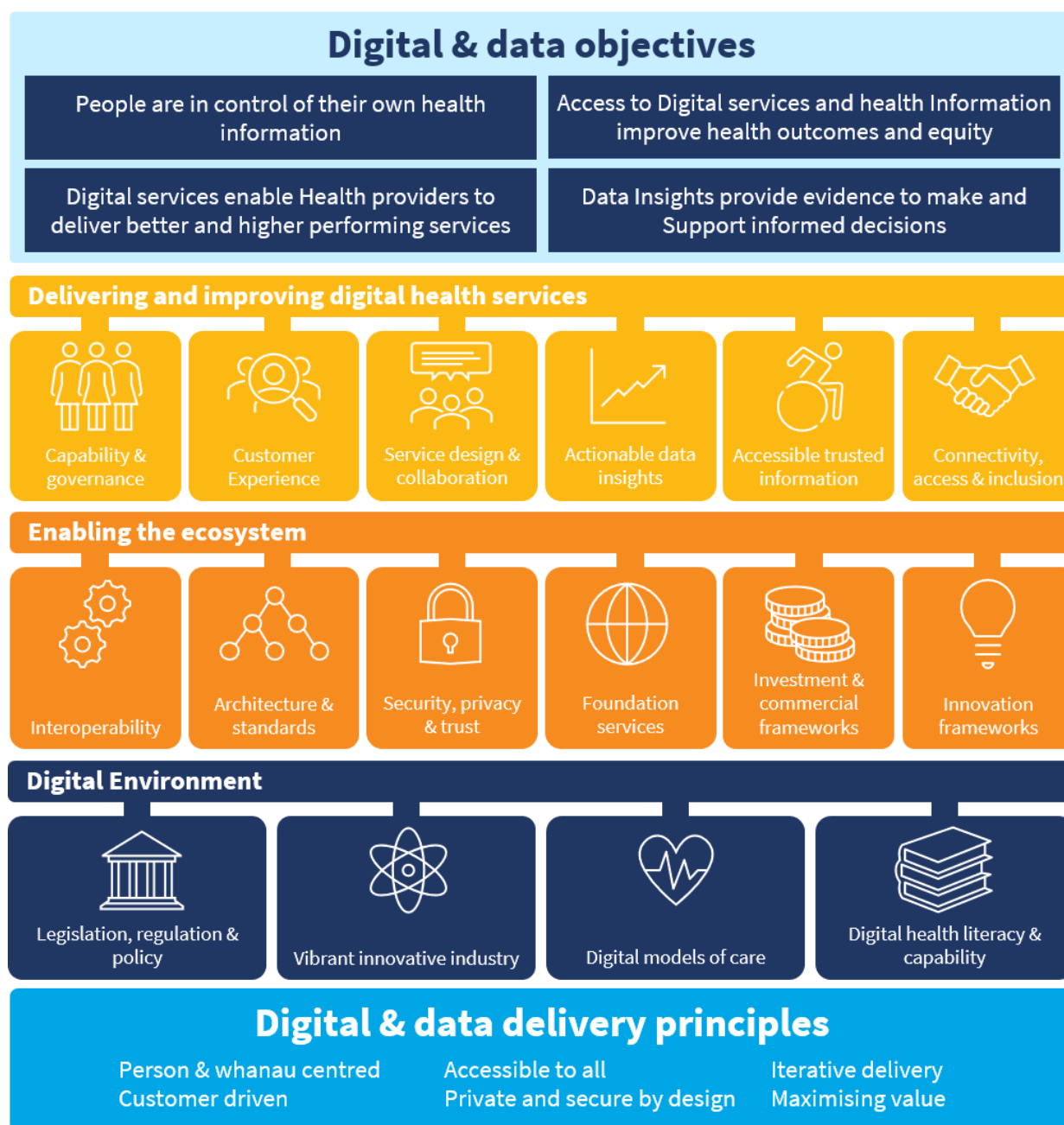
It is essential that the strategy is sufficiently **broad and deep**. Breadth refers to incorporating the four main data types: health care, public health, social care and long-term care data. Depth ensures that all data are included, and that they can be linked at the individual level to enable better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

An important accompaniment to the digital strategy are roadmaps for each strategic objective, particularly those that will be challenging to achieve, such as data interoperability. The roadmaps should be specific about who is responsible for what and when deliverables can be expected. The roadmaps should address the full breadth and depth of the strategy to ensure a balanced and coherent strengthening of the Dutch health information system. Hence not only enhancement of interoperability and secondary use of data in clinical care but inclusion of data uses in public health, long term care and social care.

Figure 4.1 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 4.1. New Zealand Digital Health Strategic Framework



Source: Ministry of Health, New Zealand (2020^[1]), "Digital Health Strategic Framework", <https://www.health.govt.nz/our-work/digital-health/digital-health-strategic-framework>.

A national strategy will require leadership and expertise

The Ministerie van Volksgezondheid, Welzijn en Sport (VWS) 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 MHWS should lead the development of a national strategy. In doing so, the MHWS should:

1. Build trust and support for the strategy among stakeholders and the public.

- Consult with governmental agencies (Informatie Beraad, IGJ, ZIN, NZa) on needs for information, analytics and information products.
- Consult with non-government stakeholders especially patient groups, regions and municipalities, provider organisations, health professional groups, insurers, academia, biomedical industry and software vendors.
- Develop and implement a public information campaign, public consultations and other avenues for public input into the strategy.
- Conduct public consultations at all stages of development of the national health data governance framework and provide public information, such as a website, to disseminate information about the development process and its outcome, as part of the National Strategy.
- Launch a government campaign with communication experts to promote a dialogue with the public about the benefits of data sharing and exchange, with the goal of valuing health data in the Netherlands as a public good (see below).
 - This public dialogue must assuage public and stakeholder concerns about privacy risks and reassure them by clearly communicating about how privacy will be protected when data are used.

2. Draft the high-level IT architecture/infrastructure for an integrated health information system that meets the information needs of key stakeholders.

- Review existing architectures within and outside of the Netherlands and improved architectures proposed in the academic literature.
- Review existing data exchanges to co-ordinate, integrate and ensure the exchange meets the needs of all stakeholders.
- Review and recommend global standards for data exchange and semantic interoperability, taking into consideration developments and requirements within the EU.
- Include privacy-by-design protections, particularly federated learning (distributed analytics).
- Include interoperability in analytics, information and knowledge and foster the adoption of a global common data model (CDM).
- Include lifecycle interoperability to ensure analytical uses of historical data as the information system evolves (i.e. ensure health trajectories and longitudinal data analysis are supported).

3. Further develop and strengthen the national health data governance legislative framework to support the national strategy. The framework must align with European regulations and should specify the following.

- The requirements for uniform data standards for health terminology, data exchange, interoperability and a common health data model.
- The requirements for the exchange, access to and use of data to serve the health-related public interest.
- The requirements for data security and privacy protection by design ('privacy-by-design').

4. Lead the legislative and policy reforms necessary to realise the strategy, in consultation with other areas of government where needed.

- Draft the role and mandate of the national authority responsible for the implementation, maintenance, and oversight of the integrated health information system (see next section for detailed functions of such an authority).
- Develop policy tools and financial incentives to realise the strategy.

5. Develop the draft roadmaps for each strategic objective within the national strategy.

- Ensure that the roadmaps are specific regarding who is responsible for each step and when results can be expected.

Role of the MHWS in the implementation of the integrated health information system:

- Ensure the MHWS oversees the national agency and is engaged in strategic planning and strategic decision-making (see the next section regarding the role of the national agency).
- Evaluate and publicly report on progress in the implementation of the national strategy.
- Facilitate progress in policy and legal reforms to support the on-going development of the integrated health information system in consultation with the national agency and the Informatieberaad Zorg.
- Develop and maintain analytics products and dashboards for ministerial policy making and reporting.
- Co-ordinate planning and funding of health information projects within the ministry to align them with the strategy.
- Develop campaigns and tools to improve public transparency about health information, information governance and public benefits from improvements in health information.
- Review planning and funding of health information projects within the ministry to ensure they align with and contribute to the strategy and do not detract from or create disincentives to advance the strategy.

Key competencies to develop and implement the strategy:

- Strategic planning of health information projects,
- Evidence-based indicator development and policy analysis,
- Informatics (IT architecture, data exchange standards, semantic interoperability),
- Health data science (statistical and software development competencies, interoperability of analytics),
- Legislative frameworks,
- Privacy-by-design (privacy protection, data security and related information technology competencies), and
- Public consultation and communications/public relations.

Aligning with a broader national digital strategy

Considering the general nature of developing the strategy for an integrated health information system, incorporating it into a broader national strategy will be an advantage. In fact, most countries that are successfully digitalising their health systems have a national digital strategy – and data governance – that encompasses all areas of public policy including health. Estonia, for example, decided over two decades ago to become a ‘digital society’ meaning that 99% of public services, including health care are accessible virtually.¹ This has paid not only immense dividends during the COVID-19 pandemic, enabling the country’s

health, education and welfare systems to continue to function as normal, it has also promoted technological and policy advances in privacy and digital identity, made Estonia into Europe's top entrepreneurial hotspot according to the World Economic Forum.²

Several Dutch experts and stakeholders interviewed emphasised their preference for need for a general national digital or data strategy. Some mentioned the approach taken in the field of education (i.e. SURF). Others mentioned initiatives of Municipalities and the Ministry of Internal Affairs which include social care data. In addition to the obvious synergies, the advantages of a cross-sector approach are particularly strong in the health arena given the value placed on privacy and security, the key role of non-health data (which can greatly enhance knowledge-generation), and the fact that makes a country more attractive for investment of biotech capital.

Institutional functions to develop, implement and oversee an integrated health information system

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 health care providers, software vendors and other developers of IT solutions. This will require a range of functions and competencies that are currently absent, without legal mandate or dispersed across various agencies in the Dutch health data landscape. These functions can be assigned to existing key institutions or be taken on by a new agency.

A national agency to implement and oversee the health information system

A single agency will be needed to co-develop and implement the national strategy and oversee/maintain the resulting health information system. This could be done by 'strengthening' or combining expertise of existing organisations 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. Consider the roles of similar national agencies in Portugal and Estonia from Chapter 2. The national agency should also develop the national platform for public data exchange, acting as a hub through which the data flows to support secure access to and use of health data to serve the public interest. Consider the role of the French Health Data Hub, the Finnish FinData, the Australian DataPlace and the EU Health Data Space discussed in Chapter 2.

Many OECD countries have separate organisations responsible for national health data and for national electronic health record systems (see Chapter 2). This legacy has been problematic wherever there were no formal structures requiring the separate organisations to work closely together toward a common goal of enabling the secure primary and secondary use of health data. Working closely together is difficult because, for example, when tackling similar tasks, health statisticians and researchers within health data organisations differ from health informatics experts in both working methods and even in the vocabulary used to discuss the task. Further, the working methods and vocabularies of experts in health data privacy and security are more closely aligned with the legal community and are different from both health informatics and health statistics and research professionals. An integrated health information system is therefore dependent upon the effective integration of functions and of different professional groups who bring critical skills together to fulfil these functions.

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 an advisory body for development and maintenance of technical standards.

The role of this authority would be responsible for standardisation, certification, a national public data platform and stakeholder consultation and engagement.

1. Standardisation: Agreeing (or developing) and maintaining consistent national standards and keeping standards for:

- Semantics (terminology),
- Electronic messaging (exchange),
- Analytics (common data model, code sharing/analytics pipeline),
- Data accessibility/sharing (prevent information blocking, secure (privacy-protective) data access, patient portals, health data space), and
- Harmonisation of data privacy and security policies and practices including national guidance for health data processors.

2. Certification and verification of compliance with national standards

- Certifying vendors of IT solutions and digital tools for compliance with national standards.
- Certifying and verifying health care providers and other information system actors have achieved interoperability standards and are exchanging useable (quality) data and are not blocking data. This process must go beyond simply demonstrating that standards are used. Proof of data interoperability (exchange, data quality) should also be required to achieve certification.

3. Building and maintaining a national public data platform for data exchange, acting as a hub through which the data flows to:

- Enable effective and secure processing of personal health data including data integration/linkage,
- Foster adoption of a common health data model (CDM),
- Manage the approval process for data integration and access requests involving data from multiple organisations,
- Enable effective and secure mechanisms for access to personal health data for approved purposes, such as approved research,
- Improve data quality, including conducting data quality auditing, and
- Reduce overlapping and duplicative administrative and data processing activities among key stakeholders within the health information system.

4. Stakeholder engagement and consultation to develop engagement in and support of the implementation of the national strategy through:

- Stakeholder and Public consultation about the national strategy and its implementation, and
- Public transparency about the national strategy and the development, exchange, uses and data privacy and security protections of health data.

Governance of the national agency

The governance of the national agency requires consideration of the role such governance will play in effecting a change in the culture toward co-operation in health data development and exchange and in valuing health data as a public good.

To increase the buy-in and support for the agency and its mandate to implement the national strategy, it will be important to ensure that the national agency seeks the advice of and listens closely to the needs of all relevant stakeholder groups, such as the groups represented within the Informatieberaad Zorg today and health data infrastructure organisations, holders of key national health data, and health and medical

research institutes and businesses who contribute to and depend upon the health information system, such as representatives of pharmaceutical, medical device, data analytics, data applications and EHR system businesses. A potential advisory body is an expanded Health which is discussed further below.

The formal governance of the national agency must be appropriate to the Dutch context and culture. Consider, however, how frequently stakeholders will be engaged in advising the agency and the effort they will expend to do so and ensure that these organisations will realise a win-win from their participation.

Key competencies of the national agency:

- Strategic planning and management of health information projects,
- Evidence-based indicator development and policy analysis,
- Informatics (IT architecture, data exchange standards, semantic interoperability),
- Data science/analytics (statistical analysis, database architecture, coding, machine learning, distributed analytics, common data models, open science/code sharing),
- Systems testing, data quality checks and software evaluation including certification,
- Web and mobile applications development (websites, web portals and smartphone apps),
- Privacy by design (privacy protection, data security and related information technology competencies), and
- Public consultation and communications/public relations.

Technical infrastructure and standards

A key role of the new agency will relate to the technical infrastructure needed for an integrated health information system. Several requirements will also require attention, particularly if the system is to be retrofitted to the existing health system.

To facilitate information development and analytics, it will be necessary in many cases to re-code existing data to a common data model (CDM). Leading global health data models, such as the OMOP (Observational Medical Outcomes Partnership) CDM, should be selected for this purpose and the technical capacity instituted.

Similarly, modern IT architecture and global 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, informatics and data science is again emphasised.

The Informatieberaad Zorg as an advisory body to the national agency

A potential advisory body for developing and implementing the national strategy is already in place, the Informatieberaad Zorg. This body currently lacks a formal mandate and is missing participation from key organisations with responsibility for national health information and who contribute to and depend upon the health information system. Furthermore, its focus is presently on primary use of clinical data hence the needed broadening (to other sectors like public health, long term care and social care) and secondary data use needs to be reflected in either the composition of the IC or another mechanism of representation of stakeholders to assure an integrated health information system for the health system as a whole. 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.

The Informatieberaad Zorg could become a forum of reflection and advice to the government and to the national agency. Specifically, its role would principally concern:

- Advising on the development and implementation of the national strategy for an integrated health information system, and
- Acting as ambassadors and spokespersons for the national strategy.

Membership of the Informatieberaad Zorg

Representatives within all key stakeholders in an integrated health information system, including organisations participating in the existing IC and new members representing organisations with responsibility for national health information (including health care, public health, social care and long-term care data); national health care quality registries; national health research infrastructures; organisations providing national health data access, linkage and governance; and businesses who contribute to and depend upon the health information system, such representatives of pharmaceutical, medical device, data analytics, data applications and EHR system businesses.

Members of the Informatieberaad Zorg should have executive or decision-making power within their respective organisations to provide strategic advice to the national agency on matters that may impact upon their organisations.

Implementation will hinge on governance, policy as well as trust

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 the implementation capability of the national agency, and will primarily comprise developing new legislation, guidelines, governance, and funding mechanisms.

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.

Building trust

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 (See Box 4.1).

Box 4.1. Building Trust

Building trust among stakeholders and the public is an important aspect of health data governance and an effective data infrastructure. A lack of trust will undermine efforts to exchange data for primary and secondary purposes. First and foremost, trust is achieved through actions not words. Rhetoric must be matched by visible acts and changes to the status quo. It is a challenging process. While trust is established over a long time (years not months), it can be lost very quickly.

Any campaign to establish trust (and it should be approached as a campaign) should be based on transparency and inclusion. All stakeholders need to be part of developing and designing the change – in this case the strategy – from the beginning. Consultation on the finished product, developed by experts, will not achieve this. An iterative consultation process on the national strategy comprising 2 to 3 steps may take longer but will ensure people trust the finished product because *inter alia* they will have a sense of ownership and are invested in its success.

Transparency is key for establishing trust and for maintaining it. Key decisions, challenges, problems and resolutions should be communicated, and lines of accountability made clear. Successful countries have created public websites where people can access information about the strategy and everything concerning health data, its use, how it is managed and secured, how privacy is protected as well as the outputs of various programmes and projects that use personal health data.

Using health data to serve the public interest should be framed as an opportunity, not a risk. The long list of benefits should be explained in detail, using real-world examples. Every stakeholder group should be made aware how the changes will benefit them. For example: patients stand to receive modern health services, higher quality care and access to better, safe treatments; providers will have better data and information to improve practice and deliver high quality care; public health officials will have timely and complete information about infectious disease outbreaks, real-time data on vaccine safety and effectiveness, granular data to guide policies for managing NCDs; payers stand to access more detailed information on health care activity, costs and outcomes; policy makers will be better able to assess how the system performs and regulate it more intelligently; industry will have a tremendous resource to spur invention and technology; and society will benefit from an innovative and agile health sector that not only delivers the best possible outcomes but attracts investment and contributes to economic growth.

This way, the conversation can shift to a more complete view where NOT using data is a risk health and prosperity, and the discussion becomes how this can be done safely and securely. It is therefore crucial to be upfront about privacy, how it is secured, and how problems or failures are resolved. In fact, transparency is critically important when things don't go to plan. Nothing destroys trust faster than bad news being hidden. Equally, timely and clear communication about how past problems have been resolved can have a reassuring effect.

Finally, public education and PR campaigns need to be intelligently planned and rolled out. Engagement of professional expertise from advertising and communications are advised. Prominent 'champions' and thought-leaders from various walks of life should be co-opted to be part of the campaign promote the strategy. Alongside health and data science experts, it can be helpful to employ public figures (actors, musicians, footballers) to communicate the message. Getting the PR campaign wrong can have consequences. In 2014, the United Kingdom mailed out paper pamphlets to inform the public about health data governance under the care.data project. The campaign failed to get the public's attention and when public concerns about care.data arose later on they included the reaction that public consultation and communication about care.data were inadequate.

Source: OECD (2015^[2]), *Health Data Governance: Privacy, Monitoring and Research*, <https://dx.doi.org/10.1787/9789264244566-en>.

The key will be to allocate sufficient time and resources to 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.

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.

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 one national interpretation of 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 health care funding and remuneration that reward care co-ordination and value will affect the functioning of an integrated health information system.

References

- Ministry of Health, New Zealand (2020), *Digital Health Strategic Framework*, [1]
<https://www.health.govt.nz/our-work/digital-health/digital-health-strategic-framework>.
- OECD (2015), *Health Data Governance: Privacy, Monitoring and Research*, OECD Health Policy [2]
 Studies, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264244566-en>.

Notes

¹ <https://e-estonia.com/>.

² <https://www.weforum.org/agenda/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/>.



From:

Towards an Integrated Health Information System in the Netherlands

Access the complete publication at:

<https://doi.org/10.1787/a1568975-en>

Please cite this chapter as:

OECD (2022), "Towards an integrated health information system in the Netherlands", in *Towards an Integrated Health Information System in the Netherlands*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/44f43851-en>

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and 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. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at <http://www.oecd.org/termsandconditions>.