



# Health at a Glance 2023

OECD INDICATORS



# Health at a Glance 2023

OECD INDICATORS

# Table of contents

Foreword	3
Reader's guide	9
Executive summary	13
<b>1 Indicator overview: Country dashboards and major trends</b>	<b>17</b>
Introduction	18
Health status	20
Risk factors for health	22
Access to care	24
Quality of care	26
Health system capacity and resources	28
To what extent does health spending translate into better health outcomes, access and quality of care?	30
<b>2 Digital health at a glance</b>	<b>33</b>
Introduction	34
Framework for digital health readiness assessment	36
Indicators of digital health readiness	40
Assessing digital health as a determinant of health	54
Concluding thoughts	56
References	56
Notes	58
<b>3 Health status</b>	<b>61</b>
Life expectancy at birth	62
Trends in all-cause mortality	64
Main causes of mortality	66
Avoidable mortality (preventable and treatable)	68
Major public health threats	70
Mortality from circulatory diseases	72
Cancer mortality	74
Chronic conditions	76
Maternal and infant mortality	78
Mental health	80
Self-rated health	82

<b>4 Risk factors for health</b>	<b>85</b>
Smoking	86
Alcohol consumption	88
Illicit drug use	90
Diet and physical activity	92
Overweight and obesity	94
Environment and health	96
<b>5 Access: Affordability, availability and use of services</b>	<b>99</b>
Population coverage for healthcare	100
Unmet needs for healthcare	102
Extent of healthcare coverage	104
Financial hardship and out-of-pocket expenditure	106
Consultations with doctors	108
Digital health	110
Hospital beds and occupancy	112
Hospital activity	114
Diagnostic technologies	116
Hip and knee replacement	118
Ambulatory surgery	120
Waiting times for elective surgery	122
<b>6 Quality and outcomes of care</b>	<b>125</b>
Routine vaccinations	126
Cancer screening	128
Safe prescribing in primary care	130
Avoidable hospital admissions	132
Diabetes care	134
People-centredness of ambulatory care	136
Safe acute care – workplace culture and patient experiences	138
Safe acute care – surgical complications and obstetric trauma	140
Mortality following acute myocardial infarction (AMI)	142
Mortality following ischaemic stroke	144
Patient-reported outcomes in acute care	146
Care for people with mental health disorders	148
Integrated care	150
<b>7 Health expenditure</b>	<b>153</b>
Health expenditure in relation to GDP	154
Health expenditure per capita	156
Prices in the health sector	158
Health expenditure by financing scheme	160
Public funding of health spending	162
Health expenditure by type of service	164
Health expenditure on primary healthcare	166
Health expenditure by provider	168
Capital expenditure in the health sector	170

<b>8 Health workforce</b>	<b>173</b>
Health and social care workforce	174
Doctors (overall number)	176
Doctors (by age, sex and category)	178
Geographic distribution of doctors	180
Remuneration of doctors	182
Nurses	184
Remuneration of nurses	186
Hospital workers	188
Medical graduates	190
Nursing graduates	192
International migration of doctors and nurses	194
<b>9 Pharmaceutical sector</b>	<b>197</b>
Pharmaceutical expenditure	198
Pharmacists and pharmacies	200
Pharmaceutical consumption	202
Generics and biosimilars	204
Pharmaceutical research and development	206
<b>10 Ageing and long-term care</b>	<b>209</b>
Demographic trends	210
Life expectancy and healthy life expectancy at age 65	212
Self-rated health and disability at age 65 and over	214
Dementia	216
Safe long-term care	218
Access to long-term care	220
Informal carers	222
Long-term care workers	224
Long-term care settings	226
Long-term care spending and unit costs	228
End-of-life care	230

# **2** Digital health at a glance

---

OECD countries are struggling to maximise the value from digital health because technologies and the data environment are often outdated and fragmented. This chapter explores the concept of digital health readiness – assessing the policy, analytic, technical and social environment that enables successful use of digital health. The concept of readiness is taking on increased urgency with the realisation that digital health is an emerging determinant of health. The chapter first looks at the policy components of an integrated digital health ecosystem to establish dimensions of digital health readiness – analytic, data, technology and human factor readiness. It then compiles and analyses indicators to measure readiness in these dimensions. The chapter concludes with a brief exploration of digital transformation as a determinant of health, providing some examples of the benefits of digital health in acute care to lower costs and improve the patient experience.

---

## Introduction

Digital tools and the use of health data are transforming how health services are delivered, how public health is protected, and how chronic conditions are managed and prevented. Digital health<sup>1</sup> is playing an ever-increasing role in health systems through electronic health records (EHRs), the use of population health data for monitoring and policy, and the integration of digital tools such as telemedicine into routine clinical care. An integrated approach to digital health also supports the responsible use of artificial intelligence (AI) and analytics, by sharing quality health data through secure technical connections across all modes of care and administration. Digital transformation has been described as a determinant of health, as digital technologies, access, and literacy increasingly influence health, well-being and health transformations.

OECD countries are striving to realise the potential of digital health while minimising possible harms. While health has been slower than other sectors of the economy to leverage the potential of digital transformation, the COVID-19 pandemic has accelerated change. However, there are still significant barriers to overcome for countries to be ready for digital transformation. For example, health systems continue to rely on fax machines, with 75% of global fax traffic used for medical services (Gintux, 2023<sup>[1]</sup>); life-saving innovations are discovered, but it can take 17 years for published leading practice to become common practice (Morris, Wooding and Grant, 2011<sup>[2]</sup>); health providers express concern over their new digital burden while not receiving benefits from modern technologies (OECD, 2019<sup>[3]</sup>); and the public cannot engage meaningfully in their care without access to their own health records.

Meanwhile, the digital landscape is complicated by the different stakeholders involved. Alongside public systems, some large multi-national private sector entities offer specific interventions, such as subscription models for integrated care that, without suitable regulation, create data silos. Conflicting, uncoordinated systems of health data use and access risk health systems being unaware of inequities and preventing the utilisation of data for public health protection and health system improvement.

Through the pandemic, the eyes of the public and policy makers were opened to the necessity of timely and quality data to inform evidence-based policy making during the crisis. The public began to engage with their own health data and providers virtually, and learned a new language of statistics, R-values, positive testing rates and vaccinations. The pandemic furthered interest in health data privacy, security and governance, in addition to opportunities for innovative analytics. For example, digital health enabled:

- Canada, Latvia, Spain, the United Kingdom and the United States to scale up remote disease management and monitoring;
- Costa Rica, the Czech Republic, Finland, Latvia, Spain and the United States to improve care co-ordination and integration;
- Australia, Austria, the Czech Republic, Luxembourg and Spain to improve electronic prescribing.

Governance, legal, and regulatory changes are necessary to support adaptation to a digital health future without loss of protections for the public (OECD, 2023<sup>[4]</sup>). In early 2023, with the backdrop of increased attention to ChatGPT, the potential of AI caught public interest and concern. There are opportunities for AI in health – from automating administrative processes to aiding health professionals in diagnosis, powering medical devices for improved treatment, virtually testing millions of antibiotics for superbugs, and discovering new methods to prevent or better treat chronic conditions. There are also risks with, but not always caused by AI, including biased algorithms that exacerbate inequities, lack of clinical validation that risks patient safety, and potential for privacy breaches.

At the same time, with greater reliance on digital health are growing risks of cyberattacks. Some project that the cost of cyberattacks (across all industries) may reach USD 10.5 trillion by 2025 (Forbes, 2023<sup>[5]</sup>). Health is a prime target for cybercrime given the sprawl of health technologies, the value of health data, and the risk of disruption in health services from technical outages.

Most countries are pursuing these opportunities while addressing risks through the implementation of digital health strategies. These strategies acknowledge the importance of taking the lessons learned from the COVID-19 pandemic and providing better health services and outcomes for the public, while addressing the digital divide. There is an opportunity for investments in digital strategy to generate potential returns of USD 3 for every USD 1 of investment. These returns come from improved health outcomes, reduction of waste, and minimised duplication, while also supporting more resilient health systems (OECD, 2019<sup>[3]</sup>).

Countries' ability to recognise the above factors in health data systems and to develop infrastructure, strategies, and governance frameworks to use in improving health systems is a signal of "digital health readiness". This is a measure of the ability to make use of analytics, data, and technology for beneficial individual, community, and public health outcomes. Digital health readiness is the foundation from which data can be leveraged for primary and secondary uses to improve well-being, health outcomes, and resilience.

This thematic chapter examines countries' digital health readiness "at a glance", with a focus on indicators of readiness to realise benefits from digital health while minimising its harms. These indicators are not exhaustive; nor are all indicators specific to the health sector. The chapter provides the groundwork for a more comprehensive approach to a robust suite of digital health indicators for readiness. While data are not currently available across all dimensions of digital health readiness (Box 2.1), this chapter details the dimensions of a framework and signals the need for more regular data collection and policy discussions about the indicators. Looking forward, it may be appropriate to consider aspects of integration with social data (e.g. social determinants of health, social programme usage) for an overall view of health and well-being.

### Box 2.1. Definition of digital health and dimensions of digital health readiness

Despite the increased importance of digital health, consistent terminology is elusive; this impairs cross-border collaboration and prevents scaling of innovation for better health outcomes. The scope of digital health can be limited to the type and use of digital technologies; it could be focused on improvement of healthcare delivery; or it could be a strategy for fulsome health system transformation (HIMSS, 2020<sup>[6]</sup>).

The *Global Strategy on Digital Health 2020-25* of the World Health Organization (WHO) brings together primary uses of digital tools with secondary uses for populations and the public. A connection between secondary generation of insights and their use in healthcare, promotion, and prevention creates a continuous improvement cycle that benefits everyone (WHO, 2021<sup>[7]</sup>).

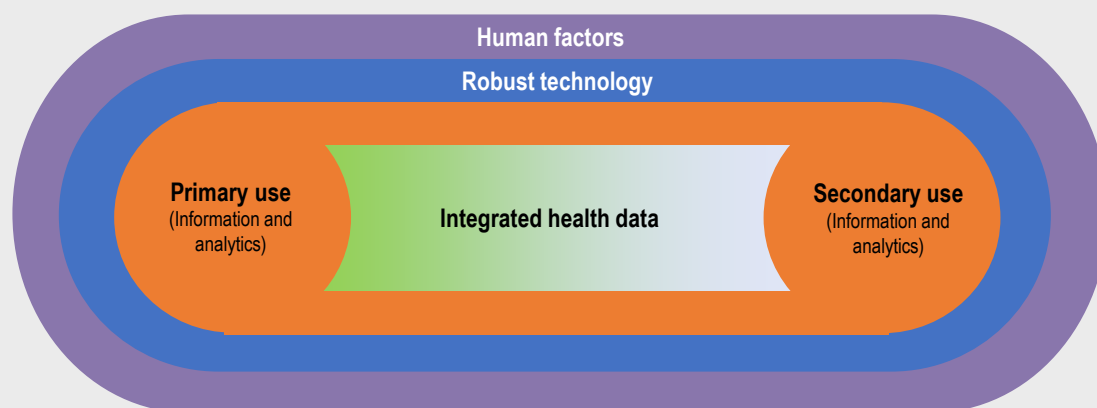
As such, digital health readiness provides a foundation for primary uses (e.g. by clinicians and patients for care, and by individuals for their agency) and secondary uses (e.g. for population health, health system continuous improvement, public health, and research and innovation). Building on the WHO definition, this document defines digital health as follows (with added parts in **bold**):

*The field of knowledge and practice associated with the development and use of **health data and digital technologies** to improve health. Digital health expands the concept of eHealth to include digital consumers, with a wider range of smart devices, connected equipment, **and digital therapeutics**. It also encompasses other uses of **data and digital technologies** for health such as the Internet of things, artificial intelligence, big data and robotics, **and predictive and prescriptive analytics**. **Analytics can be for health system improvement, public health preparedness, or research and innovation.***

In this context, the dimensions of digital health readiness include **analytic readiness** (for responsible analytics); **health data readiness** (for integrated health data); **technology readiness** (for robust technology); and **human factor readiness** (for capacity, co-operation, and oversight). Collectively, these need to be designed to work together to optimise health outcomes while minimising harms.

When responsible analytics, integrated health data and reliable technology are brought together, they form an **integrated digital health ecosystem**.

Figure 2.1. Integrated Digital Health Ecosystem



Source: Sutherland, E. (forthcoming<sup>[8]</sup>), "Policy checklist for integrated digital health ecosystems".

The chapter first outlines the dimensions of digital health readiness across analytics, health data and technology, as well as the human factors that provide trust, coherence, and sustainability. Indicators are mapped to a subset of components – with some proxy measures – to analyse the performance of OECD countries within the framework.

Second, the chapter discusses the indicators and their findings through the dimensions of digital health readiness, which include analytic readiness, data readiness, technology readiness, and human factor readiness. The chapter further identifies countries that perform well consistently across the chosen digital health readiness indicators.

Third, the chapter looks at sample health outcomes and their relationship with dimensions of readiness to explore digital health readiness as a determinant of health. Further, this chapter discusses examples and opportunities to evaluate the relationship between digital health readiness and effects on costs and health outcomes.

Finally, the chapter summarises findings from the first three sections. It concludes with a call for further work on developing measures of digital health readiness to improve understanding of its relationship with positive health outcomes, lower costs, and higher levels of innovation.

## Framework for digital health readiness assessment

The performance of digital health is not as easy to measure as indicators in other chapters in *Health at a Glance*, as it is both a new discipline and one that is constantly changing. The issue is exacerbated by the somewhat elusive definition of digital health (as discussed in Box 2.1).

Digital health readiness is a measure of the ability to make use of analytics, data, and technology for beneficial individual, community, and public health outcomes. Hence, “readiness” is a composite of abilities and structures across analytics, data, and technology. In addition, readiness requires human factors outlined above for capacity, co-operation, and oversight. Dimensions of digital health readiness are categorised as follows:

- **Analytic readiness** assesses the readiness for analytics to be created and used to generate action that improve health outcomes for individuals, communities, and the public. The objective of analytic readiness is responsible analytics that are trusted and inform equitable health outcomes. In health, this includes readiness to develop and deploy responsible AI to help doctors and nurses in their routine tasks (e.g. documenting cases) or diagnostics (e.g. interpreting radiology images).
- **Data readiness** assesses the readiness for data to be collected, accessed, and used in analytics. The objective of data readiness is integrated and quality health data that are available for healthcare, public health, health system improvement, research, and innovation. For example, data readiness includes policies that enable data protection, de-identification, access, and linking to help improve the safety of health systems.
- **Technology readiness** assesses the readiness for technology to support the secure input, storage, and movement of data. The objective of technology readiness is robust technology that is resilient to digital security risks and technology outages while maintaining data integrity. This includes aspects of technical interoperability that, when combined with semantic interoperability, allow health systems to communicate with each other with high data quality and timeliness.
- **Human factor readiness** assesses the readiness of the digital health ecosystem (including analytics, data, culture, and technology) to achieve its objectives with sufficient resources and to be resilient to shocks. The objective of human factor readiness is to foster trust among stakeholders, acquire sufficient financial and human resources, encourage co-operation and re-use for mutual benefit, and adapt to emerging issues and challenges. Included in this is digital health literacy to ensure that the public, providers, and policy makers have the knowledge necessary to use the digital health ecosystem effectively, including its necessary protections.

Collectively, a health system that has high digital health readiness is designed to optimise positive health outcomes while minimising harms from analytic, data, or technology misuse. High digital health readiness is aligned with OECD legal instruments for artificial intelligence (AI), health data governance, and digital security, and digital identity (see Box 2.2).

## Box 2.2. OECD legal instruments and digital health readiness

### Health data governance

In 2017, OECD countries endorsed a Recommendation on Health Data Governance that encourages adoption of a national health data governance framework, 12 components of that framework, and co-operation on definition and implementation of interoperability standards.

In practice, the Recommendation covers a broader perspective around digital health, all of which contributes to digital health readiness. The table below maps which parts of the Recommendation apply to which parts of digital health readiness, noting that all areas are ultimately required for digital health.

Recommendation on health data governance	Dimensions of digital readiness
Engagement and participation of stakeholders in the development of a national health data governance framework	Human factors
Co-ordination within government and co-operation among organisations processing personal health data to encourage common data-related policies and standards	Human factors
Reviews of the capacity of public sector health data systems to serve and protect public interests	Human factors
Clear provision of information to individuals about the processing of their personal health data including notification of any significant data breach or misuse	Technology
The processing of personal health data by informed consent and appropriate alternatives	Data
The implementation of review and approval procedures to process personal health data for research and other health-related public interest purposes	Data
Transparency through public information about the purposes for processing of personal health data and approval criteria	Human factors
Maximise the development and use of technology for data processing and data protection	Technology
Mechanisms to monitor and evaluate the impact of the national health data governance framework, including health data availability, policies, and practices to manage privacy, protection of personal health data and digital security risks	Human factors
Training and skills development of personal health data processors	Human factors
Implementation of controls and safeguards within organisations processing personal health data including technological, physical, and organisational measures designed to protect privacy and security	Data Technology
Requiring that organisations processing personal health data demonstrate that they meet the expectations set out in the national health data governance framework	Human factors

Source: OECD (2016<sup>[9]</sup>), Recommendation of the Council on Health Data Governance, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433>.

### Artificial Intelligence (AI)

In 2019, the OECD published value-based principles for AI. These apply to the development of AI, although they are appropriate for general practices in analytics.

The principles for AI are consistent with and complementary to the OECD Recommendation on Health Data Governance.

Recommendation on artificial intelligence	Description	Dimensions of digital readiness
Inclusive growth, sustainable development, and well-being	Stakeholders should proactively engage in responsible stewardship of trustworthy AI in pursuit of beneficial outcomes for people and the planet	Analytic
Human-centred values and fairness	AI actors should respect the rule of law, human rights, and democratic values, throughout the AI system lifecycle	Analytic
Transparency and explainability	AI actors should commit to transparency and responsible disclosure regarding AI systems	Analytic
Robustness, security, and safety	AI systems should be robust, secure, and safe throughout their entire lifecycle so that – in conditions of normal use, foreseeable use or misuse, or other adverse conditions – they function appropriately and do not pose unreasonable safety risk	Analytic
Accountability	AI actors should be accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles and the context, and consistent with the state of the art	Analytic

Source: OECD (2019<sup>[10]</sup>), Recommendation of the Council on Artificial Intelligence, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

## Digital security

In 2022, OECD countries endorsed a Recommendation on Digital Security Risk Management that provides a set of nine principles for digital security and encourages OECD countries to adopt national approaches to digital security risk management. These will help to minimise the risk of successful cyberattacks and the impacts if an attack should be successful.

The principles for digital security risk management are consistent with and complementary to the OECD Recommendation on Health Data Governance.

Recommendation on digital security risk management	Description	Dimensions of digital readiness
Digital security culture: awareness, skills, and empowerment	All stakeholders should create a culture of digital security based on an understanding of digital security risk and how to manage it	Technology
Responsibility and liability	All stakeholders should take responsibility for the management of digital security risk based on their roles, the context, and their ability to act	Technology
Human rights and fundamental values	All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values	Technology
Co-operation	All stakeholders should co-operate, including across borders	Technology
Strategy and governance	Leaders and decision makers should ensure that digital security risk is integrated in their overall risk management strategy and managed as a strategic risk requiring operational measures	Technology
Risk assessment and treatment	Leaders and decision makers should ensure that digital security risk is treated based on continuous risk assessment	Technology
Security measures	Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk	Technology
Resilience, preparedness and continuity	Leaders and decision makers should ensure that a preparedness and continuity plan based on digital security risk assessment is adopted, implemented, and tested, to ensure resilience	Technology
Innovation	Leaders and decision makers should ensure that innovation is considered	Technology

Source: OECD (2022<sup>[11]</sup>), Recommendation of the Council on Digital Security Risk Management, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479>.

## Governance of Digital Identity

In June of 2023, the OECD adopted Recommendations on the Governance of Digital Identity. These aim to support domestic approaches to digital identity that are user-centred and trusted.

The recommendations on digital identity are consistent with and complementary to the OECD Recommendation on Health Data Governance.

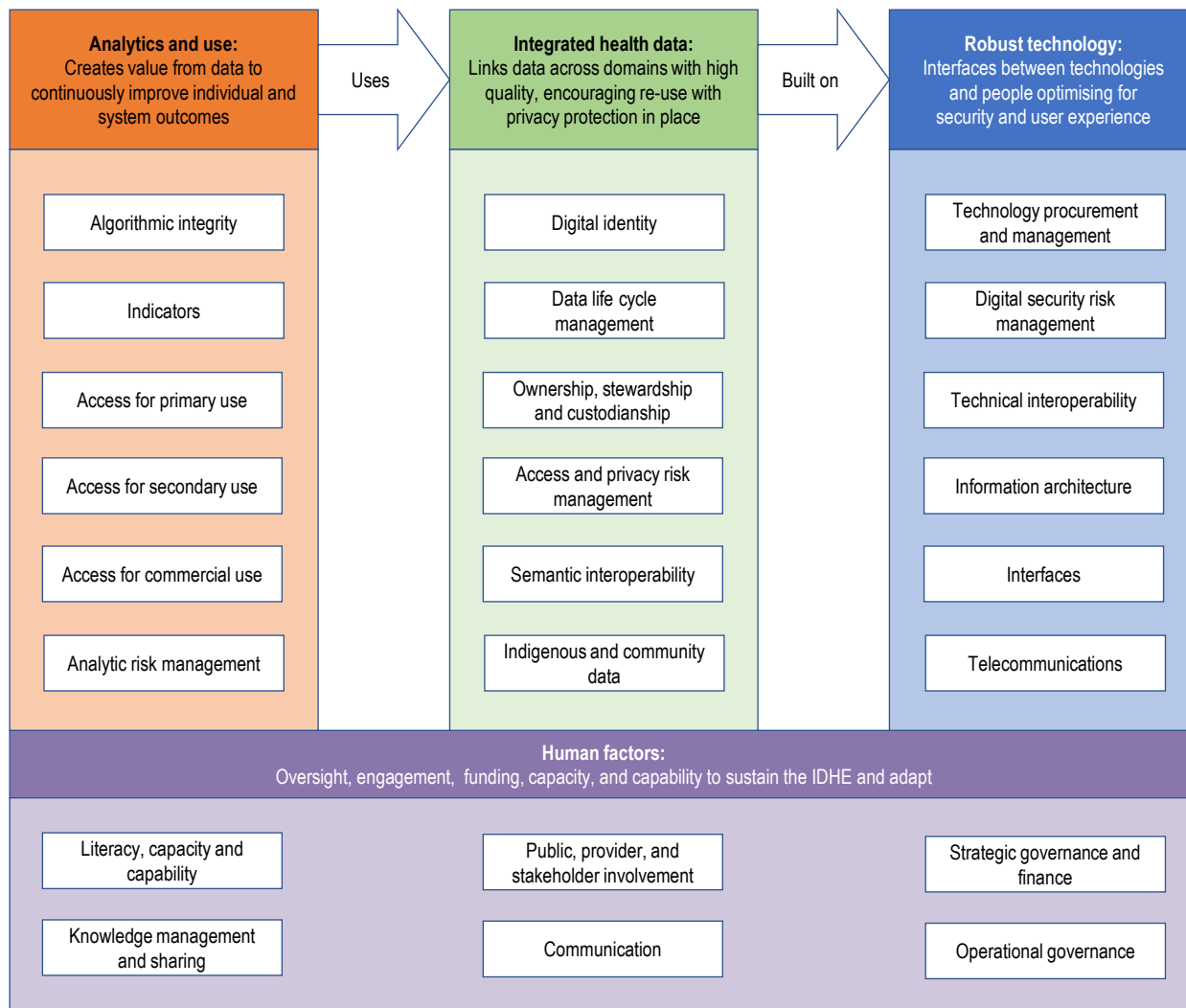
Recommendation on digital identity	Description	Dimensions of digital readiness
User-centred and inclusive digital identity systems	Designing and implementing digital identity systems that are effective, usable, and responsive to the needs of users and service providers, while prioritising inclusion, reducing barriers to access, and preserving non-digital ways to prove identity	Data
Strengthening the governance of digital identity	Defining roles and responsibilities and align legal and regulatory frameworks across the digital identity ecosystem(s). Protecting privacy and prioritising security to ensure trust in digital identity systems	Data
Cross-border use of digital identity	Co-operating internationally to establish the basis for trust in other jurisdictions' digital identity systems and issued identities. Understanding needs of users and service providers in different cross-border scenarios	Data

Source: OECD (2023<sup>[12]</sup>), Recommendation of the Council on the Governance of Digital Identity, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491>.

Digital health readiness is the foundation for primary and secondary uses of data and technology across all sectors of healthcare delivery and management. When considerations of the links to and from other parts of the digital health ecosystem and the readiness of the environment to support their long-term, sustainable use are lacking, the result is fragmented solutions that cannot be integrated.

Understanding the policies required for a digital health ecosystem will help to guide the selection of indicators for digital health readiness that support the ability to integrate solutions into broader policies for care, safety, and system effectiveness. In systems with high digital health readiness, these policies should be designed together to orchestrate activities across analytics, data, and technology; this also reduces overlap and avoids policy inconsistencies or contradictions. Figure 2.2 represents a checklist of policies for digital health ecosystems.

**Figure 2.2. Checklist of policies for an integrated digital health ecosystem (IDHE)**



Source: Sutherland, E. (forthcoming<sup>(8)</sup>), "Policy checklist for integrated digital health ecosystems".

As digital health readiness is a fundamental component of an efficient and modern health system, efforts should be made to facilitate regular capture and analysis of appropriate indicators to monitor it. Ideally, digital health readiness would have indicators for each of the policy areas in Figure 2.2. These could start by measuring the existence of the relevant policy and evolve into indicators that measure the effectiveness of implementation of that policy. Currently, there is no comprehensive capture of such indicators. Table 2.1 includes a set of initial measures of digital health readiness. Proxies have been used where direct data are not available. Most proxies are not specific to health.

**Table 2.1. Initial indicators for digital health readiness including proxy measures**

Dimension of digital health readiness	Associated policy area	Indicator or proxy presented in this chapter	Comment
Analytic readiness	Access for primary use	Dataset availability, maturity and use score (OECD)	
	Access for secondary use	Patient access to their own health data (OECD)	
	Algorithmic integrity	Global AI Index (third party)	Proxy measure
Data readiness	Data lifecycle management	Dataset governance score (OECD)	
	Digital identity	Digital Government Index (OECD)	Proxy measure
	Semantic interoperability <i>Technical interoperability</i>	Interoperability standard adoption (OECD)	Should extend to semantic data standards
Technology readiness	Internet availability	Internet connectivity for individuals (OECD)	For entire population
	Digital security	Digital security (OECD)	
	Technology procurement	Certification of vendors (OECD)	
Human factor readiness	Strategic governance	Digital health strategies (various)	
	Literacy, capacity and capability	Digital skills in Europe (third party)	Proxy measure
	Public, provider and stakeholder involvement	Digital citizen engagement index (third party)	Proxy measure

These indicators are presented in more depth in the next section.

## Indicators of digital health readiness

Digital health is emerging as an essential component of health systems, with recent literature indicating that digital transformation is a determinant of health (The Lancet Digital Health, 2021<sup>[13]</sup>). To manage digital health better, it is necessary to measure the effectiveness and efficiency of the creation of analytics, data, and technology. This will help to strengthen the foundations of healthcare for the digital age.

This section reviews each of the dimensions of readiness defined in the above section based on the indicators from Table 2.1. These indicators are an incomplete view of readiness for digital health; however, they may provide inspiration for future work to better define comprehensive indicators and support routine data collection. Such work would also help to identify leaders in digital health (to share expertise) as well as gaps where there is mutual benefit in collaboration.

### **Analytic readiness indicators**

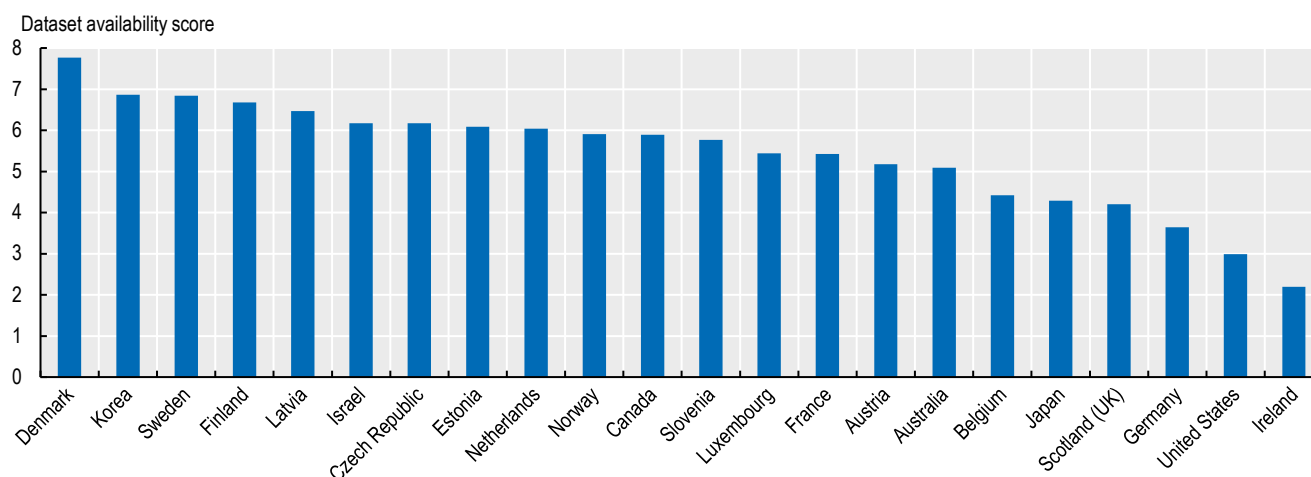
Analytics are the part of digital health that generates value for people, communities, and society. This value is generated in diverse ways – for example, by providing better precision healthcare for individuals, addressing health inequities for marginalised communities, protecting the public from health emergencies, supporting more effective health monitoring and financing policies, and discovering new life-saving innovations.

Three areas that are essential for analytic readiness are the ability to access and link data for healthcare and secondary use, the ability for individuals to access their own data, and the ability to apply analytic techniques, as with AI.

#### *Ability to access and link data – primary and secondary uses*

The readiness to create meaningful analytics and ensure their appropriate use is dependent on timely access to quality data and the ability to link data across datasets. Primary uses of these data are for healthcare whenever and wherever necessary – across primary care, acute care, and individual data use. Secondary uses of data include patient safety, public health preparedness, health service management and planning, health system improvement, and research and innovation.

In 2022, the OECD performed a five-year review of the Recommendation on Health Data Governance (OECD, 2016<sup>[9]</sup>). This reported on capabilities to link and use data across critical data domains. The score for analytic readiness demonstrated wide variation among OECD countries (see Figure 2.3).

**Figure 2.3. Ability to access and link datasets in healthcare**

Note: Lithuania and Spain have reported this capability, but no data were available in the survey when it was conducted.

Source: OECD (2022<sup>[14]</sup>), *Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance*, <https://doi.org/10.1787/68b60796-en>.

The dataset availability score is a composite indicator that incorporates eight measures including:

- timely data access that covers the national population across care settings and clinical registries;
- use of interoperable clinical data standards and identifiers that enable linking across datasets;
- use of linked data for primary and secondary health purposes.

In this indicator, Denmark had the highest composite score, followed by Korea, Sweden, Finland and Latvia. Denmark scored highest in seven of the eight measures: the country reported that data were extracted from electronic records for all key datasets, coded using clinical data standards, covering more than 80% of the population, and linkable by a unique patient identifier. Further, linked data were used for healthcare quality, performance, research, and monitoring. Only Latvia scored higher than Denmark on timeliness of data, with a greater percentage of data available for use within one week. Korea performed similarly to Denmark, except for linking a registry for cardiovascular disease with other data. Sweden also performed similarly, except for linking primary care data and only having one dataset available within one week of the original data creation at source.

#### *Ability to access and link data – individual use*

Both the OECD Recommendation on Health Data Governance (OECD, 2016<sup>[9]</sup>) and WHO's Global Strategy on Digital Health 2020-2025 (WHO, 2021<sup>[7]</sup>) call for individuals to have access to their own health records. With this access, individuals will be more knowledgeable about the state of their well-being. It will facilitate conversations with health providers as the individual will no longer need to remember their prior vaccinations, prescriptions, test results, or medical treatments. In more advanced EHR systems, the individual can contribute information to their health record to report on symptoms, correct errors, or progress with health treatments.

In 2021, the OECD published a Survey of Electronic Health Record System Development, Use and Governance. This showed variation in availability of portals, the ability to access all records, and the ability to interact with data. The findings are summarised in Table 2.2.

Almost 90% of responding OECD countries reported having an electronic portal in place; however, only 42% reported that the public could both access and interact with all their data through the portal. Fewer than half of responding countries indicated that all patients could access their data via portals.

Denmark, Italy, Lithuania, Luxembourg and Türkiye reported having a portal for patients to access their comprehensive health data that was available to their entire population. Further, their portals allowed patients to interact with their data.

**Table 2.2. Patient access to and interaction with their own EHRs through a secure internet portal**

Access via portal Access to ALL records Interaction with portal	Access via portal Access to SOME records Interaction with portal	Access via portal Access to ALL records NO interaction with portal	NO access via portal
11			
Australia			
<b>Denmark</b>	9		
Germany	Belgium		
<b>Italy</b>	Canada		
<b>Lithuania</b>	Costa Rica		
<b>Luxembourg</b>	Czech Republic		
Netherlands	<b>Finland</b>		
Slovenia	<b>Iceland</b>	3	3
Sweden	<b>Israel</b>	<b>Estonia</b>	Korea
Switzerland	Portugal	Hungary	Mexico
<b>Türkiye</b>	United States	<b>Japan</b>	Norway

Note: Countries in **bold** reported that 100% of patients are covered. Some OECD countries, like the Netherlands, use multiple EHR portals. Spain also has this capability, but no data was available in this survey.

Source: Slawomirski, L. et al. (2023<sub>[15]</sub>), "Progress on implementing and using electronic health record systems: Developments in OECD countries as of 2021", <https://doi.org/10.1787/4f4ce846-en>.

### *Artificial Intelligence (AI) and algorithmic integrity*

Readiness of analytics is also dependent on integrity of the methods used to create the analytics. This issue has gained more prominence owing to increased awareness of the potential benefits and risks of AI. AI holds the potential to revolutionise healthcare by improving diagnostics, helping with development of new treatments, supporting providers, and extending healthcare beyond the health facility and to more people. Projections have suggested that the use of AI could lead to vaccines against cancer and cardiovascular and autoimmune diseases by the end of this decade (The Guardian, 2023<sub>[16]</sub>). AI is already being used to find new antibiotics (McMaster University, 2023<sub>[17]</sub>). However, AI also has significant risks due to potential biases and lack of transparency of the algorithms created. Implementation of AI has both the potential to help address issues of equity and the potential to expand inequities.

Broad measures of AI are not yet available, although there are indications of which countries are leading AI development and implementation. A Global AI Index (Tortoise, 2023<sub>[18]</sub>) measures implementation, innovation, and investment in AI across all sectors, including health and private sectors, and provides a country ranking. The Index covers 62 countries, including 36 OECD countries (all except Costa Rica and Latvia). Table 2.3 presents the rankings for the top ten countries.

**Table 2.3. Top ten countries in the Global AI Index**

Country	Talent	Infra-structure	Operating environment	Research	Development	Government strategy	Commercial investment	Overall score
<b>United States</b>	1	1	28	1	1	8	1	1
China	20	2	3	2	2	3	2	2
Singapore	4	3	22	3	5	16	4	3
<b>United Kingdom</b>	5	24	40	5	8	10	5	4
<b>Canada</b>	6	23	8	7	11	5	7	5
<b>Korea</b>	12	7	11	12	3	6	18	6
<b>Israel</b>	7	28	23	11	7	47	3	7
<b>Germany</b>	3	12	13	8	9	2	11	8
<b>Switzerland</b>	9	13	30	4	4	56	9	9
<b>Finland</b>	13	8	4	9	14	15	12	10

Note: Countries in **bold** are OECD countries.

Source: Tortoise (2023<sub>[18]</sub>), Global AI Index, [www.tortoisemedia.com/intelligence/global-ai/](http://www.tortoisemedia.com/intelligence/global-ai/), latest data available from June 2023.

The United States leads the Index overall, with seven other OECD countries in the top ten. The United States leads in five of seven dimensions (talent, infrastructure, research, development, and commercial investment). Denmark leads in operating environment. Germany is the leading OECD country in government strategy (second overall where Saudi Arabia is first).

Given the accelerated growth of AI, it is likely that this will be an area of significant interest – to realise its benefits while protecting against its risks – in years to come. Several entities have started work on regulation of AI, including the European Union (EU) (via the proposed Artificial Intelligence Act), Canada (via the proposed Artificial Intelligence and Data Act), and the United States (via the blueprint for an AI Bill of Rights).

While none of these advances are specific to health, the sector has significant risks and opportunities from AI. Risks include hidden biases and lack of transparency that may result in inappropriate clinical recommendations that lead to patient harm. Security and privacy risks are also associated with training and use of AI, given the breadth of data required for effective training of the algorithms.

Nevertheless, there are also significant benefits of AI use in health, such as:

- **relieving health workforce pressures** by using AI to automate administrative tasks – estimated to improve productivity by 10% (Beamtree, 2023<sup>[19]</sup>);
- **augmenting clinical diagnoses** by pulling information from unstructured doctor notes to bring issues to the surface, which has led to better diagnoses for breast cancer patients who would otherwise have fallen between the cracks (Petch et al., 2023<sup>[20]</sup>);
- **detecting public health emergencies** by using AI to scan global health activity to detect unusual patterns of concern so that public health leaders can be informed as quickly as possible to formulate an appropriate response (CNBC, 2020<sup>[21]</sup>).

Countries are actively working to understand how to achieve benefits from AI across their health systems while minimising risk. A critical area to address in the rollout of AI will be its social acceptance. Studies in the United States and Canada have indicated that patients want doctors to be the face of care and do not want to be diagnosed by a machine (OTV NEWS, 2023<sup>[22]</sup>; Pew Research Center, 2023<sup>[23]</sup>). This is consistent with the OECD AI Principle of human-centredness values and fairness (OECD.AI, n.d.<sup>[24]</sup>).

### **Data readiness indicators**

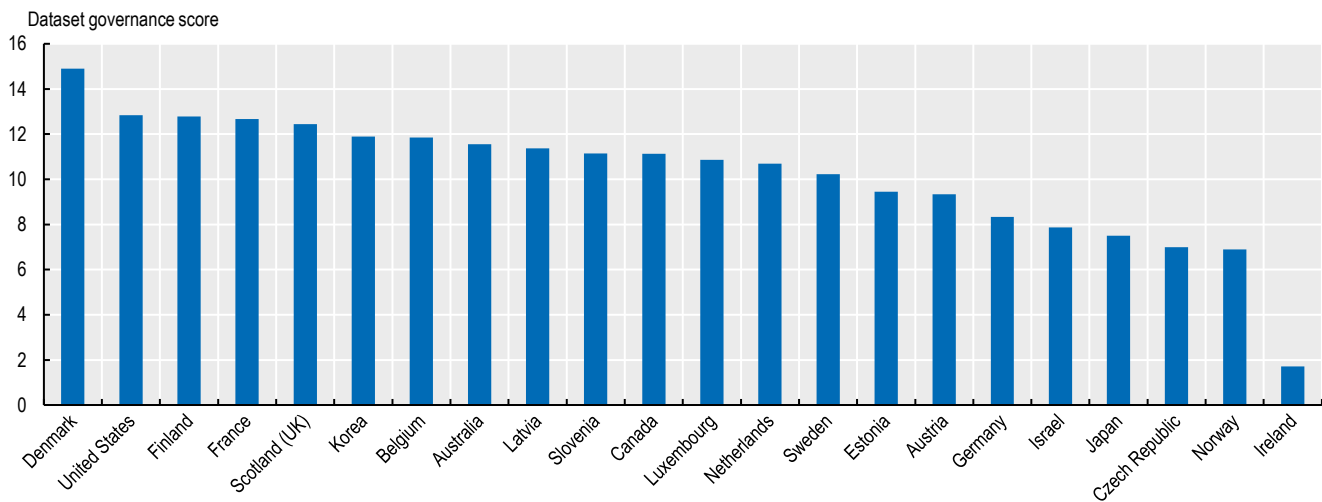
The full value of analytics can only be unlocked if quality data are available, with necessary protections in place to ensure that data are secure and private. Countries that are ready to use data understand that harms may come both from sharing data (e.g. from privacy breaches) and from not sharing data (e.g. missed drug interactions, lack of awareness of growing inequities, inability to manage chronic conditions).

Three areas that are essential for data readiness are governments' approaches to the governance of health data, digital transformation of systems, and interoperability.

#### *Governance of health data (lifecycle management)*

The readiness to collect, store, and provide access to quality data is dependent on having clear structures and policies in place that define accountabilities, provide clear guidance for decision making, and support trust among health organisations and the public.

In 2022, the OECD performed a five-year review of the Recommendation on Health Data Governance (OECD, 2016<sup>[9]</sup>), which included a score for dataset governance (see Figure 2.4).

**Figure 2.4. Dataset governance in healthcare**

Note: Score calculated as a sum of proportions of national healthcare datasets with recommended governance elements (see source).

Source: OECD (2022<sup>[14]</sup>), *Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance*, <https://doi.org/10.1787/68b60796-en>.

The dataset governance score is a composite indicator that incorporates 15 measures including:

- training and operational controls for privacy and security;
- processes for data-sharing arrangements;
- data catalogues and their contents.

In this indicator, Denmark had the highest composite score, followed by the United States, Finland, France and Scotland (United Kingdom). Denmark scored highest in 14 of 15 measures (including equal scores): the country reported that legislation authorises creation of datasets with data protection officers in place; staff are trained on data protections and their access to data is controlled; standard data-sharing agreements are in place for data sharing within the public sector, with academics, with the private sector and across borders, where data are de-identified/pseudonymised prior to sharing; access may be gained through remote means or through research data centres; and dataset descriptions are made public with their legal basis, along with clear procedures for data linkage. Only the United States scored higher than Denmark on the measure of testing the risk of re-identification. The United States had similar scores to Denmark, scoring highest in 11 of 15 measures, with opportunities to expand cross-border data sharing, to include the legal basis for the dataset publicly and to link long-term care data. Finland scored highest in 13 of 15 measures but had areas of improvement to measure re-identification risk and increase research data centre access.

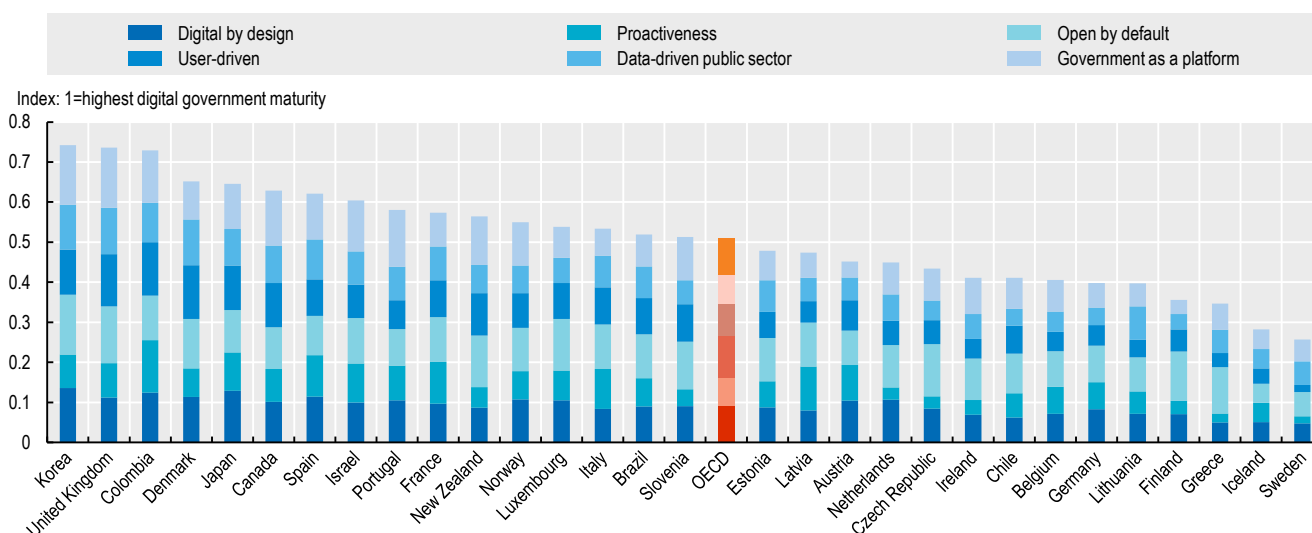
#### *Digital Government Index for digital identity*

The readiness of data is also determined through government policies as part of a drive for overall digital transformation. As an input to the OECD's Going Digital programme, 31 countries were evaluated in a Digital Government Index in 2019 (OECD, 2019<sup>[25]</sup>). This measured six attributes:

- **Digital by design** assesses the governance and adoption of digital technologies to rethink and re-engineer public processes, simplify procedures, and create new channels of communication and engagement with stakeholders.
- **Data-driven public sector** measures the extent to which governments value data as a strategic asset and establish governance, access, sharing and re-use mechanisms for improved decision making and service delivery.
- **Government as a platform** benchmarks the extent to which governments deploy shared platforms, standards, and services to help teams focus on user needs in public service design and delivery.
- **Open by default** measures the degree of openness of government data and policy-making processes available to the public, within the limits of existing legislation and in balance with national and public interests.
- **User-driven** assesses the extent to which user needs are considered in the design of policies and services, including using inclusive mechanisms (e.g. dedicated service design mechanisms or digital tools to understand users' needs).
- **Proactiveness** benchmarks the level of anticipation of governments to attend to people's needs and respond to them rapidly, avoiding the need for cumbersome data and service delivery processes.

The OECD Digital Government Index is presented in Figure 2.5.

**Figure 2.5. OECD Digital Government Index (2019)**



Source: OECD (2019<sup>[25]</sup>), Going Digital Toolkit, <https://goingdigital.oecd.org/indicator/58>.

As of 2019, Korea was the leader in the composite Digital Government Index score, followed by the United Kingdom and Colombia. Korea led all countries in two attributes: digital by design and open by default. The United Kingdom led in the attributes data-driven public sector and government as a platform. Colombia led in proactiveness, and Denmark led in being user-driven.

While these attributes are not specific to health, they are indicative of leading practices that will be useful for health. For example, the OECD is leading work on establishment of guidelines for digital identity that allow both authentication of individuals and appropriate use and linking of their data across government services (OECD, 2023<sup>[26]</sup>).

The OECD Going Digital Toolkit includes a measure of “health data sharing intensity” (OECD, 2019<sup>[25]</sup>). In this indicator, Denmark, Finland and Norway had the highest level of data sharing – sharing data with other government bodies, universities, healthcare providers, businesses, and foreign governments – while ensuring that appropriate protections are in place (OECD, 2023<sup>[27]</sup>).

It should be noted that these measures pre-date the COVID-19 pandemic, which may have changed attitudes to health data sharing, protection, and use.

### *Interoperability standards in health systems*

Semantic data standards allow the meaning of the data to be maintained as data are transported between systems, regardless of the format, and managing differences in units. For example, sex at birth may be captured as “Male” in one system, whereas another may record it as “M”. Alternatively, a lab result for blood glucose level could be captured in units of mg/dL or mmol/L, depending on the lab. Interpreting current tests and trending results over time requires that the units be measured on the same scale.

Technical data standards support the exchange of data between technologies while the content of the data is protected. Semantic and technical standards work together, so local physical data standards are connected to each other while maintaining data quality and integrity.

There are many semantic and technical data standards in health. The OECD Survey of Electronic Health Record System Development, Use and Governance specifically examined the use of HL7-FHIR (Fast Healthcare Interoperable Resources) – a standard that focuses on technical data exchange – and SMART (Substitutable Medical Applications, Reusable Technologies) – a standard for application interfaces (Slawomirski et al., 2023<sup>[15]</sup>). A summary of the adoption of FHIR standards is included in Table 2.4.

**Table 2.4. Adoption of recent HL7-FHIR and SMART interoperability standards across OECD countries**

EHR interoperability Adopting HL7-FHIR Adopting SMART on FHIR	EHR interoperability Adopting HL7-FHIR No SMART on FHIR	EHR interoperability Not adopting HL7-FHIR No SMART on FHIR	No projects for interoperability Not adopting HL7-FHIR No SMART on FHIR
<b>10</b>			
<b>Australia</b>			
<b>Belgium</b>			
Czech Republic			
Estonia	<b>6</b>		
<b>Finland</b>	<b>Canada</b>	5	
<b>Korea</b>	<b>Denmark</b>	<b>Hungary</b>	
Lithuania	<b>Iceland</b>	Japan	3
<b>Netherlands</b>	Israel	Slovenia	Costa Rica
<b>Norway</b>	<b>Luxembourg</b>	Switzerland <sup>1</sup>	<b>Portugal<sup>1</sup></b>
<b>Sweden</b>	Italy	United States	<b>Türkiye<sup>2</sup></b>

Note: Countries in **bold** also reported working on developing public application programming interfaces (APIs).

1. Additional efforts for EHR interoperability were underway in Portugal (Adopting HL7-FHIR, no SMART on FHIR), Switzerland (Adopting HL7-FHIR and SMART on FHIR) and Spain (Adopting HL7-FHIR) though data were not captured in this survey.

2. Türkiye is implementing SMART on FHIR.

Source: Slawomirski, L. et al. (2023<sup>[15]</sup>), "Progress on implementing and using electronic health record systems: Developments in OECD countries as of 2021", <https://doi.org/10.1787/4f4ce846-en>.

Almost 90% of responding OECD countries reported that they were introducing legislation to require standards for interoperability; 66% were adopting HL7-FHIR, and 42% were adopting SMART on FHIR, which simplifies data queries, access, and exchange between systems (Slawomirski et al., 2023<sup>[15]</sup>). Australia, Belgium, Finland, Korea, the Netherlands, Norway, Spain and Sweden reported advancing a strategy for EHR interoperability, adopting HL7-FHIR standards along with SMART on FHIR, and developing application programming interfaces (API) to simplify data access and support open data.

While HL7-FHIR provides semantic data standards itself, it is compatible with semantic standards such as SNOMED<sup>2</sup> or ICD<sup>3</sup> for clinical data coding. In parallel, there are emerging approaches to semantic data standards for primary and secondary uses beyond clinical care. For primary use, the International Patient Summary (IPS) is intended as standard for both presentation of data to individuals and exchange of data across borders. Data domains required by the IPS include prescription history, allergies and intolerances, and medical diagnoses. Additional data domains include immunisation, history of procedures, medical devices, and diagnostic testing results (HealthIT.gov, 2021<sup>[28]</sup>).

For secondary use, the Observational Medical Outcomes Partnership (OMOP) Common Data Model (CDM) is an open community data standard to help interoperability of data, with a focus on secondary use. The OMOP CDM leverages the Observational Data Standards and Informatics (OHDSI) vocabularies. These models allow for standardisation across data sources for aggregate analysis. Ideally, the standards for the IPS and OMOP would work together so that data can be collected once for primary purposes and used many times for secondary use.

It should be noted that since the time of the survey (2021), interoperability standards have continued to evolve beyond HL7-FHIR and SMART. Current practice would also incorporate semantic interoperability standards, for capture and exchange of information for EHRs, as well as enabling the use of that data for secondary purposes, as discussed above. As there are yet to be surveys of adoption of the IPS or OMOP across health systems to understand the current level of readiness across semantic interoperability, subsequent measurement of interoperability will look at the adoption of policies to establish standards governance and monitor national semantic and technical data standards.

### **Technology readiness**

Technologies are intertwined with digital health – be it the user interface for a medical device, electronic medical records in hospitals that capture information, or x-ray machines that capture and share images. Readiness with digital health requires reliable technologies to collect, store, access, share and use data to produce impactful insights.

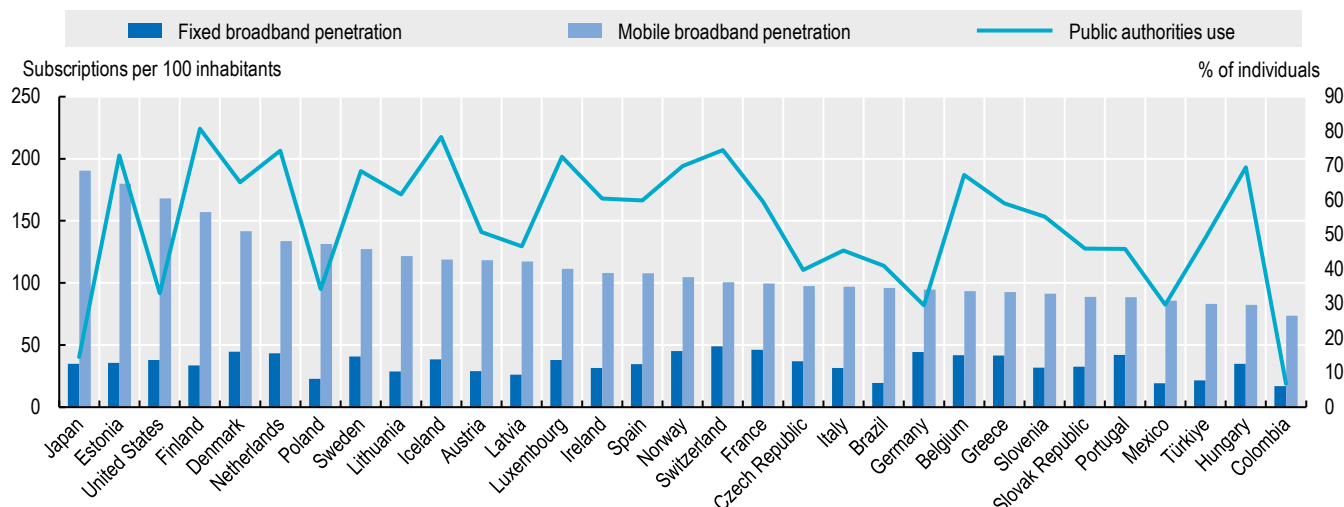
Three areas for technical readiness are the abilities of individuals to access digital tools via the internet, the security of digital systems and the approach to vendor certification.

### Internet connectivity for individuals

In an increasingly digitised world, there are calls for access to the internet to be recognised as essential for human well-being. Internet connectivity is particularly important for issues such as universal health coverage reaching remote and rural areas.

The OECD Going Digital programme measured the penetration of mobile and fixed internet connections in OECD countries and the share of individuals who used the internet to contact public authorities. A summary is presented in Figure 2.6.

**Figure 2.6. Internet use across OECD countries and use of the internet for public authorities**



Source: OECD (2019<sup>[25]</sup>), Going Digital Toolkit, <https://goingdigital.oecd.org/indicator/58>, based on the OECD Broadband Portal [www.oecd.org/sti/broadband/broadband-statistics](http://www.oecd.org/sti/broadband/broadband-statistics) and the ITU World Telecommunication/ICT Indicators Database, [www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx](http://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx).

Globally, mobile technologies are the dominant method of accessing the internet. In Japan and Estonia, there are almost two subscriptions to the internet for every individual, while the number of subscriptions is less than one per person in 12 OECD countries.

The internet is frequently used for public health purposes. In 15 OECD countries, more than 60% of the population used the internet to interact with public authorities.

As an example specific to health, more than half of citizens in Finland reported personally accessing their EHRs regularly online in 2019. They interacted with their records to renew prescriptions, update consent, post living wills, and record organ donation testaments, among other actions (Jormanainen et al., 2019<sup>[29]</sup>).

### Digital security

Digital security is a rising concern globally, with the cost of cyberattacks projected to reach USD 10.5 trillion by 2025 (Forbes, 2023<sup>[5]</sup>). The health sector is a particular target for cyberattacks because of the inherent value of health data and the extremely low tolerance for outages of digital technologies. Given the sensitivity of confidential patient data, digital health readiness requires that connections and storage are secure.

OECD countries endorsed principles for digital security risk management in 2022 that would apply across all industries (OECD, 2022<sup>[11]</sup>), as summarised in Box 2.2. These principles were used to survey approaches to digital security in health across OECD countries in early 2023. The responses were compared to leading practices and are summarised in Table 2.5.

Table 2.5. Summary of alignment of countries to leading practices for digital security

		Digital security culture	Responsibility and liability	Human rights and fundamental values	Co-operation	Strategy and governance	Security measures	Risk assessment and treatment	Innovations	Resilience, preparedness and continuity
		Digital Security Principles								
Digital Security Strategy specific to Health ( <b>bolded</b> countries identified alignment with a national digital health strategy)	<b>Australia</b>	G	G	G	G	G	G	I	G	G
	Canada	Y	Y	G	G	Y	G	Y	G	G
	Czech Republic	Y	G	Y	G	Y	G	Y	G	G
	<b>France</b>	I	I	I	I	I	I	I	I	I
	<b>Germany</b>	I	I	I	I	I	I	I	I	I
	<b>Ireland</b>	G	G	G	G	G	G	G	G	G
	<b>Israel</b>	G	G	G	G	Y	G	Y	G	G
	Netherlands	Y	Y	Y	G	Y	G	G	Y	G
	<b>Norway</b>	Y	Y	G	G	Y	G	Y	G	Y
	United Kingdom	G	G	Y	G	Y	Y	Y	Y	G
<b>United States</b>	Y	G	Y	G	Y	G	G	G	Y	
National Digital Security Strategy	Costa Rica	Y	Y	Y	G	Y	Y	Y	Y	Y
	Croatia	Y	G	G	G	Y	G	Y	G	Y
	Italy	Y	G	G	G	Y	G	G	G	G
	Japan	Y	G	G	G	I	Y	Y	I	Y
	Korea	G	G	G	G	G	G	G	G	G
	Lithuania	Y	Y	Y	G	Y	G	Y	G	G
	Portugal	Y	G	G	G	Y	G	Y	Y	Y
	Slovenia	Y	Y	Y	G	Y	G	G	G	G
	Spain	Y	G	G	G	Y	G	Y	Y	G
	Switzerland	Y	G	Y	G	Y	Y	Y	Y	G
No reported Digital Security Strategy	Belgium	Y	Y	Y	G	Y	G	G	G	Y
	Greece	Y	Y	G	G	Y	G	Y	G	G
	Luxembourg	Y	Y	G	G	Y	G	Y	G	Y
	Slovak Republic	Y	Y	G	Y	Y	G	Y	Y	G

Note: G represents 100% alignment to best practice; Y represents less than 100% alignment; 'I' represents incomplete or confidential responses.

Source: Sutherland, E. (forthcoming<sup>(30)</sup>), "Fast-track on digital security in health".

Overall, 75% of responses were aligned with the proposed leading practices. Respondents that had a specific strategy for digital security specific to health (that was aligned with a national strategy) had higher alignment with leading practices in 6.1 of the 9 principles. Respondents with a national digital security strategy were aligned with leading practices on average in 4.7 of the 9 principles. Countries without a digital security in health strategy were aligned in 4.5 of the 9 principles.

Overall, from this limited survey, it appears that Ireland and Korea are aligned with all leading practices for digital security in health. Australia, Canada, Israel and Italy also responded with strong alignment. The analysis shows some key priority areas for

government action to align with the OECD Digital Security Risk Management Framework and co-operate in areas of mutual benefit.

It is notable that some areas for improvement to mitigate digital security risks are relatively low-cost (such as training staff and monitoring programmes) when compared to extensive interventions such as advanced security solutions, security audits and penetration testing, amongst others. It is estimated that 90% of digital security challenges start with phishing. Hence, these low-cost activities could also be among the most effective.

### *Certification of technology vendors in EHR systems*

Technology vendors provide the platforms that collect, store, share, and use health data. The choice of vendor is most often made through a competitive procurement process. When technologies must be procured across a large group, a common method is to create a certification process. For a vendor to be certified, they must demonstrate that they adhere to a determined set of minimum requirements. These certifications simplify the choice of individual organisations.

For digital health readiness, a strategic approach to vendor management will help to minimise diversity of technology implementations that challenge the ability for data to be interoperable and portable. Certification simplifies the ability to share data while maintaining protections.

The OECD 2021 Survey of Electronic Health Record System Development, Use and Governance examined which common requirements were used in the certification process to examine variations in approach to vendor certification (see Table 2.6).

**Table 2.6. Certification requirements of vendors of EHR system software**

Messaging standards Clinical terminology National EHR requirements	Messaging standards Clinical terminology No EHR requirements	Messaging standards No clinical terminology No EHR requirements	No standards identified
11			
Belgium			
Denmark			9
Finland			Costa Rica
Hungary			Czech Republic
Japan			Estonia
Korea			Iceland
Portugal			Israel
Slovenia		3	Italy
Switzerland		Australia	Lithuania
Türkiye	1	Canada	Luxembourg
United States	Netherlands	Sweden	Norway

Notes: EHR requirements refers to standards for national EHR interoperability. Spain also implements standards to facilitate interoperability, but no data were available in this survey. Countries in "No standards identified" might have organisations responsible for the infrastructure of EHR software, but not necessarily setting standards for clinical terminology and electronic messaging.

Source: Slawomirski, L. et al. (2023<sup>[15]</sup>), "Progress on implementing and using electronic health record systems: Developments in OECD countries as of 2021", <https://doi.org/10.1787/4f4ce846-en>.

This survey identified significant variation across OECD countries in their certification processes. Almost 60% of OECD countries reported messaging standards as part of the certification process; however, this dropped to less than 50% for certification requiring messaging, clinical and interoperability standards. Furthermore, 38% of OECD countries reported not having any standards or not having a vendor certification process. In total, 11 countries embedded messaging standards, clinical terminology and EHR requirements in the certification process.

Given the rising importance of interoperable data and advances made during the COVID-19 pandemic, this is an area where improvement would be expected to incorporate additional interoperability standards (as discussed in the section titled Interoperability standards in health systems, and Table 2.4). There may be opportunities for international collaboration to support cross-border interoperability and data sharing for research, public safety, and health system improvement.

## Human factor readiness

While digital health is considered a technical discipline, human factors are essential for its success. As noted in the OECD publication *Health in the 21st Century* (2019<sup>[3]</sup>):

The main barriers to building digital health systems of the 21st century are not technological. They are institutional and organisational. Progress depends on an enabling policy environment.

Hence, readiness for digital health relies on the co-ordination and support of multiple actors across the health system. The health workforce and providers must understand how health information is collected and used, and – importantly – that this should support their work, not be an administrative or cultural burden. This also includes engagement and consultation to support the trust and acceptance of patients that their data are secure and private.

This section examines three areas of human factor readiness: digital health strategies, digital literacy, and meaningful public engagement.

### *Digital health strategies and strategic governance*

In 2020, the World Health Assembly endorsed WHO's *Global Strategy on Digital Health 2020-2025* (WHO, 2021<sup>[7]</sup>). The vision of the strategy emphasises equity, person-centric solutions, and integration of primary and secondary uses of data to better prepare and respond to pandemics, drive innovation to improve lives, and achieve better outcomes for everyone.

In parallel, many countries have developed national strategies for digital health to drive action (see Table 2.7).

**Table 2.7. Digital health strategies across OECD countries**

Digital health-related strategy			No digital health-related strategy found
← 35 →			
Australia	Finland		
Austria	Greece	New Zealand	
Belgium	Hungary	Norway	
Canada	Iceland	Poland	
Chile	Ireland	Portugal	
Colombia	Israel	Slovak Republic	
Costa Rica	Italy	Slovenia	
Czech Republic	Japan	Spain	
Denmark	Korea	Sweden	3
Estonia	Lithuania	Switzerland	Latvia
France	Luxembourg	United Kingdom	Mexico
Germany	Netherlands	United States	Türkiye

Source: OECD analysis from publicly available information and published national strategies.

Overall, 35 OECD countries have a strategy related to digital health, including strategies that focus on AI, health data, open data, or digital technology. All strategies address dimensions of digital health readiness (as described in Box 2.1), and the aim of all is to bolster the digital foundation of health systems.

Across these national digital health strategies, 34 articulated clear goals. Note that strategies may have multiple goals, so countries may appear multiple times in the summary in Table 2.8.

**Table 2.8. Summary of country digital health strategy goals**

Ensuring coherence between regions and operators	Supporting learning health systems	Improving resilience and sustainability	Moving towards people-centric system	Improving security and data protection	Improving productivity of health workforces	Investing in innovation	Focusing on health prevention
24	24						
Austria	Australia						
Canada	Belgium						
Chile	Colombia						
Colombia	Costa Rica						
Costa Rica	Denmark						
Denmark	Estonia						
Finland	Finland						
Germany	France						
Greece	Germany						
Hungary	Greece	14	14				
Iceland	Hungary	Austria	Denmark	13			
Ireland	Iceland	Colombia	Germany	Belgium	12		
Japan	Ireland	Germany	Greece	Czech Republic	Australia		
Korea	Israel	Iceland	Hungary	Finland	Austria		
Lithuania	Italy	Israel	Iceland	Germany	Belgium		
Netherlands	Lithuania	Lithuania	Ireland	Hungary	Czech Republic		
Norway	Luxembourg	Luxembourg	Netherlands	Israel	France	7	7
Poland	Netherlands	New Zealand	Norway	Italy	Germany	Colombia	Colombia
Portugal	New Zealand	Norway	Poland	Japan	Hungary	Denmark	Ireland
Spain	Poland	Poland	Portugal	Lithuania	Netherlands	Ireland	Israel
Sweden	Slovak Republic	Slovak Republic	Slovak Republic	Netherlands	Norway	Korea	Netherlands
Switzerland	Spain	Spain	Spain	Norway	Poland	Netherlands	Norway
United Kingdom	Sweden	Sweden	Sweden	Slovak Republic	Spain	Norway	Portugal
United States	United Kingdom	Switzerland	United States	Spain	United States	Spain	Spain

Source: OECD analysis from publicly available information and published national strategies.

More than 70% of countries identified goals to support learning health systems and improve coherence across their regions and health system operators, while approximately 41% identified improving resilience and sustainability as a priority alongside moving toward people-centric health systems. Furthermore, approximately 38% identified improving security and data protection as a priority, and 35% prioritising efforts to improve productivity of health workforces.

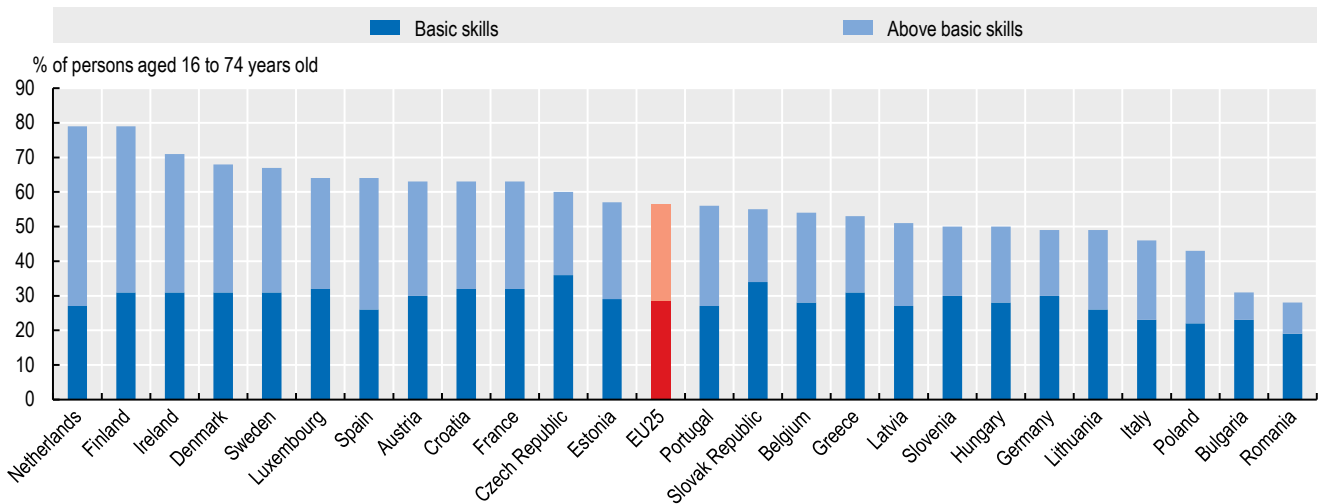
All goals rely on a foundation of digital health, where responsible analytics are created on accessible and quality data that are collected and delivered through robust technology. Notably, these strategies – while focused on digital health – would enable the transformation of the overall health system.

The presence of a comprehensive and integrated strategy signals national co-ordination and a drive to improve digital health readiness.

### *Digital skills of populations and health literacy*

Digital skills include the ability to use digital tools for communication and collaboration, problem solving, safety, digital content creation, and the comprehension and use of information. Individuals can have basic or advanced digital skills.

A recent report looked at overall digital skills in Europe (see Figure 2.7) (ILA, 2023<sup>[31]</sup>).

**Figure 2.7. Digital skills of populations in Europe**

Source: CBS, Eurostat, adapted from ILA (2023<sup>[31]</sup>), *Digital Health Literacy Country Reports*, [www.ilabour.eu/results/digital-health-literacy-country-reports/](http://www.ilabour.eu/results/digital-health-literacy-country-reports/).

This study shows that almost 80% of people in the Netherlands and Finland have at least basic digital skills, whereas fewer than 50% of people in Hungary, Germany, Lithuania, Italy and Poland have comparable digital skills.

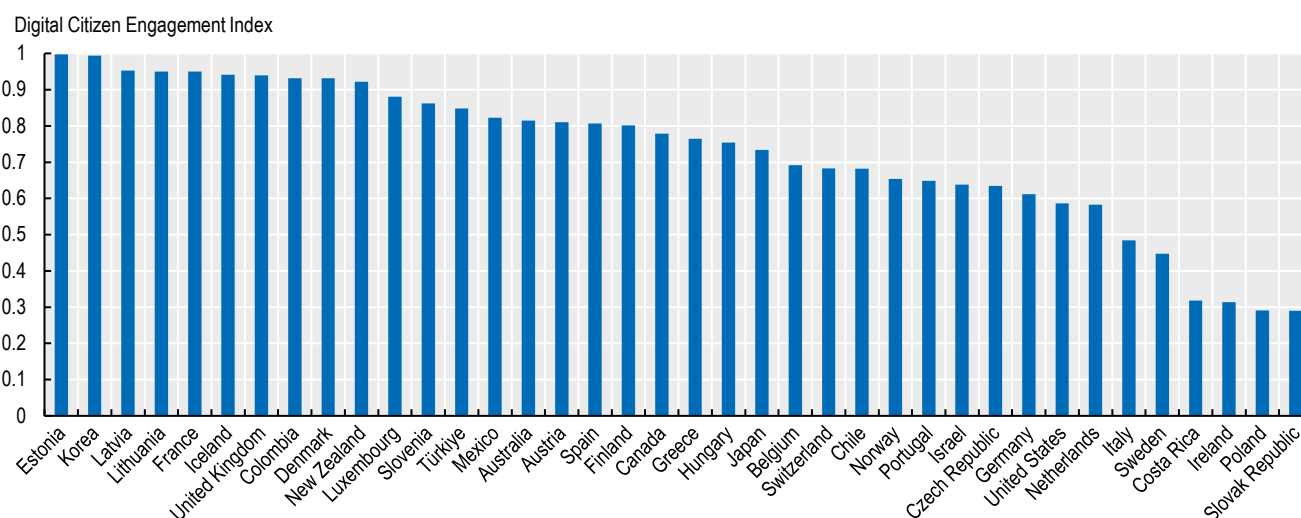
Digital health has the additional complexity of health literacy. Personal health literacy is the degree to which individuals can find, understand and use information and services to inform health-related decisions and actions for themselves and others, whereas organisational health literacy is the degree to which organisations equitably enable individuals to find, understand, and use information and services to inform health-related decisions and actions for themselves and others (CDC, 2023<sup>[32]</sup>).

Improved health literacy has been shown to improve trust among the public regarding health communications (Paige, Krieger and Stellefson, 2016<sup>[33]</sup>). Hence, actions to address both digital literacy and health literacy are important parts of digital health readiness.

### *Citizen engagement and public involvement in digital health*

People are at the centre of health in the OECD Recommendation on Health Data Governance in at least 41% of national digital health strategies (see Table 2.8 above). People being at the centre means more than ensuring that people have access to their EHRs; it also means ensuring that people are meaningfully engaged in the design, implementation, operation, and management of digital health programmes. Ways in which meaningful public engagement can be achieved include surveys, inclusion in project teams, and implementation of public assemblies.

The World Bank, as part of its work on a Governance in Technology Maturity Index (GTMI), assessed dimensions of governance including a Digital Citizen Engagement Index (see Figure 2.8) (The World Bank, 2022<sup>[34]</sup>).

**Figure 2.8. Digital Citizen Engagement Index (2022)**

Source: The World Bank (2022<sup>[34]</sup>), GovTech Maturity Index (GTMI) Data Dashboard, Accessed August 2023, [www.worldbank.org/en/data/interactive/2022/10/21/govtech-maturity-index-gtmi-data-dashboard](http://www.worldbank.org/en/data/interactive/2022/10/21/govtech-maturity-index-gtmi-data-dashboard).

Estonia and Korea have the highest scores among OECD countries, followed by Latvia, France and Lithuania. Further, 21 OECD countries are considered GovTech Leaders, indicating that these countries have a whole of government approach to public sector modernisation (including digital government transformation approaches, universally accessible public services, and a citizen-centric outlook). Strong digital citizen engagement includes having access to open data, national platforms for citizen participation, government platforms for citizen feedback, and publishing citizen engagement statistics. It should be noted that the index is not necessarily specific to healthcare and might not reflect recent changes following the COVID-19 pandemic.

Within the Digital Citizen Engagement Index, areas where fewer than 50% of OECD countries aligned with leading practices are:

- allowing citizens and businesses to provide anonymous feedback;
- responding to citizen feedback;
- making government responses publicly available;
- using advanced technology (e.g. chatbots) to improve citizen engagement;
- establishing service delivery performance metrics;
- publishing government engagement results;
- improving the representation of vulnerable groups.

There are examples of public involvement in digital health. In Canada, Patients Redefining the Future of Healthcare has created a patient declaration of health data rights that clarifies the expectation for data to be used to benefit individuals and communities while also respecting privacy (Save your skin, 2023<sup>[35]</sup>). Across the EU, the European Patients Forum has published a paper with expectations for the advancement of AI (Nicholas and del Castillo, n.d.<sup>[36]</sup>).

A third channel for meaningful public engagement is through public assemblies or citizen councils. These engage a diverse and representative group to provide advice to governments in areas of interest. In health, the United Kingdom established a public assembly in 2014 for the National Health Service (NHS). In Canada, the Health Data Research Network Canada engaged patients to understand their expectations for sharing and use of their health data. The respondents felt that: 1) identifiable health data should be shared across patients' health providers; 2) de-identified health data should be shared with policy makers for health system safety and improvement; and 3) de-identified health data should be shared with academic researchers to improve discovery and treatment of disease. These directions are helping to inform policy directions in health data sharing, privacy, and protection (HDRN Canada, 2020<sup>[37]</sup>).

### **Digital health readiness: Monitoring progress**

This section presents articulated aspects of readiness for digital health across various dimensions of analytics, data, technology, and related human factors. While this is not an exhaustive list, these initial measures of digital health readiness are helpful to identify pockets of excellence and set the stage for later work in digital readiness evaluation. Leading countries for each indicator are listed in Table 2.9.

**Table 2.9. Leading countries for indicators presented in this chapter**

Dimension of digital health readiness	Indicator or proxy presented in this chapter	Leading countries
Analytic readiness	Dataset availability, maturity, and use score (OECD)	Denmark, Korea, Sweden, Finland, Latvia
	Patient access to their own health data (OECD)	Denmark, Italy, Lithuania, Luxembourg, Sweden, Türkiye
	<b>Global AI Index (third party)</b>	United States, the United Kingdom, Canada, Korea, Israel
Data readiness	Dataset governance score (OECD)	Denmark, Finland, France, United States, United Kingdom
	<b>Digital Government Index (OECD)</b>	Norway, United Kingdom, Colombia, Denmark, Japan
	<b>Interoperability standard adoption (OECD)</b>	Australia, Belgium, Finland, Korea, Netherlands, Norway, Sweden
Technology readiness	<b>Internet connectivity for individuals (OECD)</b>	Japan, Estonia, Finland, Denmark, Netherlands
	Digital security (OECD)	Australia, Canada, Czech Republic, France, Germany, Ireland, Israel, Korea, Netherlands, Norway, United Kingdom, United States
	Certification of vendors (OECD)	Belgium, Denmark, Finland, Hungary, Japan, Korea, Portugal, Slovenia, Switzerland, Türkiye, United States
Human factor readiness	Strategic governance	<i>35 countries have a digital health-related strategy</i>
	<b>Literacy, capacity, and capability</b>	Netherlands, Finland, Ireland, Denmark, Sweden
	<b>Public, provider, and stakeholder involvement</b>	Estonia, Korea, Latvia, France, Lithuania

Note: Items in **bold** are non-health specific. Leading countries identified in the respective analyses presented earlier in the chapter, listed by ranking or alphabetical when in a top category.

Across all indicators, Denmark appears most frequently as a leading country (in 7 of 12 indicators), followed by Finland, Korea, Sweden, Japan, the United States and the Netherlands. More than 95% of OECD countries are among leading countries in at least one category (all except Mexico). This demonstrates that this is a key priority across the OECD, and that progress is being made.

Nordic countries have strength across all dimensions, appearing as leading countries in 10 of 12 indicators (all except the Global AI Index and digital security). This is bolstered by a region-specific health strategy that emphasises health prevention along with healthcare (Nordic Health 2030, n.d.<sup>[38]</sup>). Digital health will be a key component of the strategic delivery plan.

A theme in this chapter has been the inadequacy of simple-to-use indicators for digital health readiness. Measuring analytic readiness would benefit from health-specific indicators for measuring the adoption of AI at scale, while managing its risks. Data readiness would benefit from a health-specific scan of interoperability, including semantic and technical data standards as well as policies for access and privacy. Technical readiness would benefit from development of metrics for information architecture and the ability of technologies to be adaptable to change. Human factor readiness would benefit from comparison of governance models, funding mechanisms, resource allocation, digital health literacy, and trust, among other areas.

## Assessing digital health as a determinant of health

While the focus of this chapter is on assessing digital readiness, this section goes one step further by exploring digital health as a determinant of health.

During the pandemic, digital health connected testing results to policy making and measured the effectiveness of public health measures. Digital health also provided channels for providers to connect with their patients at a distance and still provide effective care. Perhaps most significantly, digital health helped to develop vaccines, evaluate their efficacy, monitor their deployment, and support a portable proof of vaccination (OECD, 2023<sup>[39]</sup>).

The *Lancet* and *Financial Times* published a Commission in 2021, highlighting that weak governance of digital technologies is causing health inequities and compromising human rights (The Lancet Digital Health, 2021<sup>[13]</sup>). However, there is yet to be a study that shows a causal quantitative relationship between digital transformation and health outcomes.

If digital health readiness is a determinant of health, then better health system performance would result in countries or organisations that have higher degrees of digital health readiness. This section shows limited examples where good digital health readiness also led to better responses to COVID-19 and improved the use of acute care resources, leading to lower costs and better patient experiences.

There are opportunities for more indicators and analysis to explore the relationship between digital health and better health outcomes, lower costs, higher innovation, and improved safety – and ultimately digital health readiness as a determinant of health.

Nevertheless, this section examines statistics for various health outcomes against digital health readiness. For these purposes, digital health readiness is taken as the multiplication of scores for dataset availability, maturity, and use (Figure 2.3) and dataset governance (Figure 2.4).

### ***Digital health and harm prevention during COVID-19***

Digital health was critical for evidence-informed policy responses during the pandemic. It was used to measure lab results to understand the extent of the disease, to support contact tracing to prevent its spread, and to optimise use of personal protective equipment to protect the most vulnerable groups (OECD, 2020<sup>[40]</sup>). Evidence-informed policies and the integration of healthcare data with public health surveillance and capacity improved infection control measures and public communication, ultimately mitigating the burden of the pandemic, and saving lives. The readiness of countries to utilise and integrate existing databases were key factors in resilient health systems (OECD, 2023<sup>[4]</sup>; de Bienassis et al., 2022<sup>[41]</sup>).

While the effects of the pandemic are still being felt, early evidence demonstrates that higher levels of digital health readiness resulted in fewer lives lost and more stable health systems during key stages of the pandemic. A comprehensive study examined the relationship between country-level digital preparedness, measured by the Digital Adoption Index (DAI), and COVID-19 cases, deaths, and stringency indices of government measures. Using linear regression on the preparedness and outcome patterns, the authors determined that **the more advanced countries' digital adoption, the lower the number of cases and the faster new cases decline**. Furthermore, gradient tree boosting analysis found the most critical factors in COVID-19 cases and deaths were related to digital infrastructure and telehealth. Overall, digital preparedness had comparable importance to smoking, age, and income on COVID-19 cases and deaths (Heinrichs et al., 2022<sup>[42]</sup>). It should be noted that the study includes low and middle-income countries who have a wider range in digital preparedness but might also have difficulties in outcomes reporting.

The rationale for this relationship is that with greater digital health readiness, policy makers were able to leverage their digital and data assets to 1) mobilise testing centres; 2) closely monitor the spread and severity of cases; 3) use results to adjust their public health measures for greater impact; 4) communicate those measures effectively; and 5) maintain service delivery through digitally-enabled care (e.g. telehealth). This could translate into reducing harms when policy makers could use results quickly to adjust public health measures for greater impact, detect where new COVID-19 cases were arising to target those areas for vaccination, and assess the efficacy of the new vaccines. Through more detailed, and OECD specific measures of digital health readiness, future analyses can examine how individual policy dimensions impact costs, outcomes, and measures of resilience in OECD countries and settings.

### ***Improving patient experience and outcomes with lower costs***

Digital health can contribute to reducing care fragmentation by integrating data across care providers. This is a key issue for people with complex health needs, such as those with multiple chronic conditions. Studies show that, without proper care integration, people may try to address unmet needs using additional services in an uncoordinated manner. This creates a sub-optimal experience for the patient and increases the risk of patient harm.

For example, estimates in the United States show that fragmented care increases costs by over USD 4 000 per patient. Further, patients who experienced high levels of fragmentation in their care were less likely to receive care considered clinical best practice (OECD, 2023<sup>[43]</sup>). In hospitals, digital health can provide a better provider experience that results in reductions in the length of hospital stays. Providers are more likely to view records when returned via electronic means and view them earlier, compared with faxed or paper records. A study (Everson, Kocher and Adler-Milstein, 2016<sup>[44]</sup>) also found that doctors were less likely to order unnecessary diagnostic tests, and patients were less likely to be admitted to hospitals, when providers reviewed the records by electronic means. Overall, patients spent less time in acute care when providers saved time between requesting and viewing outside records. Digital health contributed to lowering costs by USD 1 187 per patient while achieving better health outcomes.

Another study in the United States of several hundred hospitals correlated their digital health maturity and health outcomes. It showed that digital maturity is associated with significantly higher safety levels, better patient experiences and fewer adverse events (Snowdon, forthcoming<sup>[45]</sup>).

Finally, the United Kingdom provides an example of seeking to improve patient experiences and lower acute care utilisation. The Norfolk Community Health and Care Trust is implementing a remote-monitoring service for people living with heart and lung diseases. Patients report high satisfaction with the programme as it saves time waiting for doctors. The programme also reported a reduction in acute care admissions (NHS, n.d.<sup>[46]</sup>). More time is required to quantify the opportunity; however, preliminary results are promising.

These examples show that digital health can be a significant contributor to improved workflow in acute care settings, resulting in lower costs and better outcomes.

## Concluding thoughts

This chapter started by presenting an expanded view of digital health that includes analytics, data, and technology alongside the human factors that help to achieve sustained success. The outline of a checklist for digital health policies was used to consider measures of digital health readiness.

Indicators of digital health readiness were presented to understand the current landscape. Denmark was identified as a leader in digital health readiness, followed by Finland, Korea, Sweden, Japan, the United States and the Netherlands. Over 95% of OECD countries were a leader in at least one of the indicators shown.

The premise that digital health readiness is a determinant of health was explored, with limited – albeit interesting – findings. More indicators and analysis are necessary to qualify and quantify relationships between high digital health readiness and health outcomes. This work could be extended to consider social data (e.g. social determinants of health, social programme usage) to provide perspective on overall health and well-being.

Overall, this chapter has demonstrated that significant work is needed to better define and measure digital health readiness. With the potential benefits and risks of AI – and its reliance on all aspects of digital health – the urgency for health systems to improve their digital health readiness is clear.

Countries are “data rich and insights poor” (OECD, 2022<sup>[14]</sup>). While progress is being made to improve the use and governance of health data, there is still significant work to be done. The capacity to measure digital health readiness reliably will help policy makers identify issues that can be addressed together, evaluate the benefit of investments in digital health, and promote the urgency of digital transformation of health systems.

## References

- Beamtree (2023), *More Time To Care: Automation, Digitisation and the Workforce*, Global Impact Committee, [19]  
<https://beamtree.com.au/papers-publications/more-time-to-care/>.
- CDC (2023), *What Is Health Literacy?*, <https://www.cdc.gov/healthliteracy/learn/index.html>. [32]
- CNBC (2020), *How this Canadian start-up spotted coronavirus before everyone else knew about it*, [21]  
<https://www.cnn.com/2020/03/03/bluedot-used-artificial-intelligence-to-predict-coronavirus-spread.html>.
- de Bienassis, K. et al. (2022), “Health data and governance developments in relation to COVID-19: How OECD countries are adjusting health data systems for the new normal”, *OECD Health Working Papers*, No. 138, OECD Publishing, Paris, <https://doi.org/10.1787/aec7c409-en>. [41]
- Everson, J., K. Kocher and J. Adler-Milstein (2016), “Health information exchange associated with improved emergency department care through faster accessing of patient information from outside organizations”, *Journal of the American Medical Informatics Association*, Vol. 24/e1, pp. e103-e110, <https://doi.org/10.1093/jamia/ocw116>. [44]
- Forbes (2023), *10.5 Trillion Reasons Why We Need A United Response To Cyber Risk*, [5]  
<https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=1a085acd3b0c>.
- Gintux (2023), *The Most Surprising Fax Machine Usage Statistics And Trends in 2023*, <https://blog.gitnux.com/fax-machine-usage-statistics/>. [1]
- HDRN Canada (2020), *Social Licence for uses of Health Data: A report on public perspectives*, Health Data Research Network Canada, <https://www.hdrn.ca/en/reports/social-licence-uses-health-data-report-public-perspectives>. [37]
- HealthIT.gov (2021), *International Patient Summary*, <https://www.healthit.gov/topic/global-digital-health-partnership/international-patient-summary>. [28]
- Heinrichs, H. et al. (2022), “Digitalization impacts the COVID-19 pandemic and the stringency of government measures”, *Scientific Reports*, Vol. 12/1, p. 21628, <https://doi.org/10.1038/s41598-022-24726-0>. [42]
- HIMSS (2020), *HIMSS Defines Digital Health for the Global Healthcare Industry*, Healthcare Information and Management Systems Society, <https://www.himss.org/news/himss-defines-digital-health-global-healthcare-industry> (accessed on 25 September 2023). [6]
- ILA (2023), *Country Reports: Digital Health Literacy to Increase the Resilience of the Disadvantaged Group*, International Labour Association, <https://www.ilabour.eu/results/digital-health-literacy-country-reports/>. [31]

- Jormanainen, V. et al. (2019), "Half of the Finnish population accessed their own data: comprehensive access to personal health information online is a corner-stone of digital revolution in Finnish health and social care", *Finnish Journal of eHealth and eWelfare*, Vol. 11/4, <https://doi.org/10.23996/fjhw.83323>. [29]
- McMaster University (2023), *Scientists use AI to find promising new antibiotic to fight evasive hospital superbug*, <https://brighterworld.mcmaster.ca/articles/artificial-intelligence-new-antibiotic-drug-resistant-pathogen-acinetobacter-baumannii/>. [17]
- Morris, Z., S. Wooding and J. Grant (2011), "The answer is 17 years, what is the question: understanding time lags in translational research", *Journal of the Royal Society of Medicine*, Vol. 104/12, pp. 510-520, <https://doi.org/10.1258/jrsm.2011.110180>. [2]
- NHS (n.d.), *Remote-monitoring service for people living with heart and lung diseases reduces A&E admissions in Norfolk*, <https://www.longtermplan.nhs.uk/case-studies/remote-monitoring/>. [46]
- Nicholas, L. and J. del Castillo (n.d.), *Artificial Intelligence in Healthcare from a Patient's Perspective*, <https://www.eu-patient.eu/globalassets/report-ai-1612---del-castillo-and-nicholas-2.pdf>. [36]
- Nordic Health 2030 (n.d.), *Nordic Health 2030*, <http://nordichealth2030.org/>. [38]
- OECD (2023), "Health data sharing intensity", *OECD Going Digital Toolkit*, OECD, Paris, <https://goingdigital.oecd.org/indicator/64>. [27]
- OECD (2023), *Integrating Care to Prevent and Manage Chronic Diseases: Best Practices in Public Health*, OECD Publishing, Paris, <https://doi.org/10.1787/9acc1b1d-en>. [43]
- OECD (2023), *Online public consultation on the draft OECD Recommendation on the Governance of Digital Identity*, OECD, Paris, <https://www.oecd.org/governance/digital-government/online-public-consultation-draft-oecd-recommendation-on-the-governance-of-digital-identity.htm>. [26]
- OECD (2023), *Ready for the Next Crisis? Investing in Health System Resilience*, OECD Health Policy Studies, OECD Publishing, Paris, <https://doi.org/10.1787/1e53cf80-en>. [4]
- OECD (2023), *Recommendation of the Council on the Governance of Digital Identity*, OECD/LEGAL/0491, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491>. [12]
- OECD (2023), *The COVID-19 Pandemic and the Future of Telemedicine*, OECD Health Policy Studies, OECD Publishing, Paris, <https://doi.org/10.1787/ac8b0a27-en>. [39]
- OECD (2022), *Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance*, OECD Publishing, Paris, <https://doi.org/10.1787/68b60796-en>. [14]
- OECD (2022), *Recommendation of the Council on Digital Security Risk Management*, OECD, Paris, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479>. [11]
- OECD (2020), "The Covid-19 crisis: A catalyst for government transformation?", *OECD Policy Responses to Coronavirus (COVID-19)*, OECD Publishing, Paris, <https://doi.org/10.1787/1d0c0788-en>. [40]
- OECD (2019), *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*, OECD Health Policy Studies, OECD Publishing, Paris, <https://doi.org/10.1787/e3b23f8e-en>. [3]
- OECD (2019), "OECD Digital Government Index", *OECD Going Digital Toolkit*, <https://goingdigital.oecd.org/indicator/58>. [25]
- OECD (2019), *Recommendation of the Council on Artificial Intelligence*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. [10]
- OECD (2016), *Recommendation of the Council on Health Data Governance*, OECD, Paris, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433>. [9]
- OECD.AI (n.d.), *AI-Principles Overview*, OECD, Paris, <https://oecd.ai/en/ai-principles>. [24]
- OTV NEWS (2023), *Survey shows what Canadians think about AI tech like ChatGPT, Google Bard*, <https://www.ctvnews.ca/sci-tech/survey-shows-what-canadians-think-about-ai-tech-like-chatgpt-google-bard-1.6289326>. [22]
- Paige, S., J. Krieger and M. Stelfson (2016), "The Influence of eHealth Literacy on Perceived Trust in Online Health Communication Channels and Sources", *Journal of Health Communication*, Vol. 22/1, pp. 53-65, <https://doi.org/10.1080/10810730.2016.1250846>. [33]
- Petch, J. et al. (2023), "Developing a Data and Analytics Platform to Enable a Breast Cancer Learning Health System at a Regional Cancer Center", *JCO Clinical Cancer Informatics* 7, <https://doi.org/10.1200/cci.22.00182>. [20]

- Pew Research Center (2023), *60% of Americans Would Be Uncomfortable With Provider Relying on AI in Their Own Health Care*, <https://www.pewresearch.org/science/2023/02/22/60-of-americans-would-be-uncomfortable-with-provider-relying-on-ai-in-their-own-health-care/>. [23]
- Save your skin (2023), *Declaration of Personal Health Data Rights in Canada*, <https://saveyourskin.ca/wp-content/uploads/Declaration.pdf>. [35]
- Slawomirski, L. et al. (2023), "Progress on implementing and using electronic health record systems: Developments in OECD countries as of 2021", *OECD Health Working Papers*, No. 160, OECD Publishing, Paris, <https://doi.org/10.1787/4f4ce846-en>. [15]
- Snowdon, A. (forthcoming), *Empirical Evidence of Digital Maturity and Patient Safety Outcomes in US Hospitals*, HIMSS. [45]
- Sutherland, E. (forthcoming), "Fast-track on digital security in health", *OECD Health Working Papers*, OECD Publishing, Paris. [30]
- Sutherland, E. (forthcoming), "Policy checklist for Integrated Digital Health Ecosystems", *OECD Health Working Papers*, OECD Publishing, Paris. [8]
- The Guardian (2023), *Cancer and heart disease vaccines 'ready by end of the decade'*, <https://www.theguardian.com/society/2023/apr/07/cancer-and-heart-disease-vaccines-ready-by-end-of-the-decade>. [16]
- The Lancet Digital Health (2021), "Digital technologies: a new determinant of health", *The Lancet Digital Health*, Vol. 3/11, p. e684, [https://doi.org/10.1016/s2589-7500\(21\)00238-7](https://doi.org/10.1016/s2589-7500(21)00238-7). [13]
- The World Bank (2022), *GovTech Maturity Index (GTMI) Data Dashboard*, <https://www.worldbank.org/en/data/interactive/2022/10/21/govtech-maturity-index-gtmi-data-dashboard>. [34]
- Tortoise (2023), *The Global AI Index*, <https://www.tortoisemedia.com/intelligence/global-ai/>. [18]
- WHO (2021), *Global strategy on digital health 2020-2025*, World Health Organization, <https://apps.who.int/iris/handle/10665/344249>. [7]

## Notes

<sup>1</sup> In this chapter, "digital health" refers to the use of analytics, data and technology in healthcare, prevention and promotion. See Box 2.1 for the full definition.

<sup>2</sup> SNOMED CT or Systemised Nomenclature of Medicine – Clinical Terms is a system of medical codes, terms, etc. for clinical documentation and EHR systems. See [www.snomed.org/](http://www.snomed.org/).

<sup>3</sup> ICD or International Classification of Diseases is a widely used categorisation of diseases and medical conditions. See [www.who.int/standards/classifications/classification-of-diseases](http://www.who.int/standards/classifications/classification-of-diseases).