Annex VII. Potential market deficiencies and regulatory barriers, including a common industry-led position

Big Data and B2B platforms: the next big opportunity for Europe

Report on market deficiencies and regulatory barriers affecting the creation of EU-wide B2B health data marketplaces and unified diabetes-related datasets

EASME/COSME/2018/004

Authors: Nadina Iacob, Felice Simonelli

Table of contents

List of acronyms, abbreviations and terms

AI	Artificial intelligence
API	Application programming interface
B2B	Business-to-business
COSME	EU programme for the Competitiveness of Enterprises and Small and Medium-sized Enterprises
COVID-19	Coronavirus disease 2019
DPA	Data protection authority
DPO	Data protection officer
EASME	Executive Agency for Small and Medium-sized Enterprises
ECJ	European Court of Justice
EDPB	European Data Protection Board
eHealth	Electronic health
EHR	Electronic health record
EMA	European Medicines Agency
EU	European Union
FAIR	Findability, accessibility, interoperability, and reusability
FHIR	Fast Healthcare Interoperability Resources Specification
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
HDS	Hébergeurs de Données de Santé (French Health Data Hosting certification)
HIPAA	Health Insurance Portability and Accountability Act of 1996
ICT	Information and communication technology
IT	Information technology
mHealth	Mobile health
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
SDG	Sustainable Development Goals
SME	Small and medium-sized enterprise
SNOMED CT	Systematized Nomenclature of Medicine -- Clinical Terms
Study	Report on market deficiencies and regulatory barriers affecting the creation of EU-wide B2B health data marketplaces and unified diabetes-related datasets
T2D	Type 2 Diabetes
US	United States
WHO	World Health Organisation

Executive summary

Data-driven services and data sharing for research present a unique opportunity to **improve healthcare outcomes in the EU**. In this relatively novel field, bolstered by emerging technologies and Big Data applications, there is still significant scope for supporting data sharing and enhancing the digital health ecosystem in the EU to strengthen public health, deliver better health outcomes for citizens and promote well-being. This Study provides a comprehensive overview of the problems that impinge on the development of digital health solutions in the EU. It maps the **regulatory barriers and market deficiencies** that have so far hindered health data sharing and the creation of potential EU-wide business-to-business (B2B) health data marketplaces, with a particular focus on **Type 2 Diabetes data and unified diabetes-related datasets**. The Study relies on an extensive review of the state of the art as well as detailed input from stakeholders in the health data ecosystem.

Regulatory barriers and market deficiencies

The **main barriers and deficiencies**, that either already impede data sharing or can potentially have a negative impact on the development of the health data ecosystem, relate to: i) the regulatory framework for data protection and liability applicable across the EU; ii) the need for a trustworthy system for data sharing built on clear accountability mechanisms; iii) the need for more cooperation on common standards and enhanced data interoperability; iv) the need to ensure access to data and lift strategic barriers in the market; and finally, v) the need for digital literacy and skills to support the development of the ecosystem.

Data protection and liability. While the regulatory framework for data protection provided by the General Data Protection Regulation (GDPR) plays a central role in fostering trust and introducing a level-playing field for data protection across the EU, it also poses some challenges as health data are considered sensitive and are thus governed by more stringent rules. Member States can also introduce additional measures as they deem necessary. For businesses seeking to operate cross-border, particularly SMEs, such differences can create hurdles and translate into compliance burdens. Additionally, fragmentation is likely to occur especially considering that health law is not harmonised in the EU, and neither is contract law. The stricter measures for the protection of sensitive health data and the risk of legal fragmentation can also pose challenges to research in a cross-border setting.

Trust and accountability. Given the sensitive nature of data, health data sharing can only be effectively enabled if a trustworthy framework and accountability mechanisms are put in place. A proper level of accountability of the data controllers and processors would require that internal control systems be put in place to produce evidence that data protection and security principles are complied with (e.g. audit reports), which can be presented to data subjects, supervisory bodies, and other stakeholders. Accountability issues can be particularly problematic when it comes to mobile health solutions (such as smartphone apps), which might fail and harm the interests of patients.

Interoperability and standards. The current landscape of health data is very fragmented and characterised by incompatible IT systems, different data formats, and data silos which make it difficult to extract the full potential of data. The sheer size of the problem becomes evident when one takes into account the multiple data sources that exist (clinical data, traditional patient-generated data, digital biomarkers coming from a variety of devices, etc.) and the multiple stakeholders who interact in the field (from hospitals and patient associations to data intermediaries and research organisations). The benefits of

health data sharing can only be reaped if common data standards are adopted and common processes and systems are put in place, allowing data to flow in the ecosystem.

Strategic barriers. Companies that intend to enter the market for data-based health services may face both structural barriers (which are inherent to the digital economy and may give a competitive advantage to first movers) and strategic barriers (which can be intentionally created by existing market players to deter entry). As health data sharing is an emerging field, most of the typical strategic barriers affecting the data economy have not yet materialised in this sector; they may very well occur, however, in the future due to the ever-evolving nature of the field. To build an EU-wide health data marketplace, special attention should be paid to establishing clear and transparent rules when it comes to price and conditions to access data, to avoid unnecessary barriers and support SMEs and research.

Digital literacy and skills. Given the importance of standards, terminologies and ontologies in the healthcare sector, there is a stringent need for highly trained data scientists, developers and software engineers who can also understand and navigate the intricate landscape of medical terminologies. In addition, as digital health solutions become more widespread, there is a need – on the one hand – to train health professionals to use and prescribe digital-based therapies, and – on the other hand – to increase digital skills among individuals to ensure effective usage of novel therapies.

Policy recommendations

To **unlock the full potential of health and well-being data** – from the traditional data collected in health records to emerging biomarkers recorded through smartphones – a data-sharing framework supported by all stakeholders and rooted in trust is needed. The Study outlines policy recommendations in four key areas to bolster the development of a governance framework that can effectively support an **EU digital health ecosystem**.

1. **Reduce the costs of data sharing** by:
   - Ensuring harmonised implementation of data protection rules;
   - Limiting fragmentation due to diverging national rules;
   - Developing guidelines for anonymisation techniques compliant with the GDPR; and
   - Fostering cooperation to establish common health data standards.
2. **Increase user trust** by:
   - Defining a framework to clarify the responsibility for data quality;
   - Updating liability rules to meet the challenges of the digital transformation;
   - Establishing accountability mechanisms for increased transparency;
   - Setting up feedback loops for the sustained engagement of individuals in data sharing; and
   - Creating a 'privacy label' for apps.
3. **Foster competition and innovation** with a focus on:
   - Further enabling data portability through technical requirements;
   - Fostering interoperability to avoid indirect restrictions to accessing data;
   - Developing an EU framework for the secondary use of health data;
   - Supporting stakeholders in accessing the market; and
   - Developing clear and transparent rules for data access.
4. **Make Europeans ready for digital healthcare services** by:
   - Fostering data literacy skills in healthcare professionals and patients alike;
   - Preparing data workers with field-specific knowledge; and

- Supporting the creation of new job profiles acting as facilitators in the digital health ecosystem.

Introduction

As the COVID-19 pandemic has made clear, **reliable data** that are shared across the health ecosystem are essential for informing critical decisions, from targeted treatment and medical advice to public health policies and crisis management. The value of data is enhanced when countries cooperate and facilitate **cross-border data flows** as well as the development of **data-based services and therapies** to generate better healthcare outcomes for citizens. The EU is in the unique position to capitalise on the long-standing cooperation among Member States to support the development of a truly integrated **digital health ecosystem** that bolsters data sharing among stakeholders and across borders.

The increased use of **ICT and emerging technologies in healthcare** is seen, on a global scale, as an opportunity to improve public health, respond to epidemics and pandemics, enhance the infrastructure for effectively using health data, and promote health and well-being.[565] From this perspective, enhancing data sharing and establishing a pan-European digital health ecosystem can also contribute to achieving the **Sustainable Development Goals** (SDGs), and in particular the health targets under SGD 3 'Ensure healthy lives and promote well-being for all at all ages'.[566]

Recently, the role of **data and data sharing for innovation in the EU** has come increasingly under the spotlight. In February 2020, the European Commission laid out an ambitious digital agenda in the Communication "Shaping Europe's Digital Future",[567] underpinned by the need for seamless data flows to boost innovation in a variety of sectors and deliver benefits for citizens. The accompanying Communication "A Data Strategy for Europe"[568] outlined both the challenges that need to be overcome as well as concrete goals for enhancing data exchanges, securing more cooperation among stakeholders and supporting the creation of nine data spaces in key sectors in the EU, including a "European Health Data Space". In particular, the Data Strategy emphasised the need to improve **business-to-business (B2B) data sharing** and address the underlying problems that have prevented developments in this field such as the lack of trust, strategic barriers due to imbalances in negotiating power and limited economic incentives (such as the fear of losing competitive advantage), the fear of data misappropriation and the lack of legal clarity.[569] Such issues affect multiple sectors, but materialise in specific ways depending on the specificities of the sector at hand. To effectively support data sharing in a given sector, a thorough understanding of the specific challenges and needs of all relevant stakeholders is necessary.

---

[565] World Health Organisation (2020), Draft global strategy on digital health 2020 – 2025, Draft 27 July 2020, p. 5. Available at : https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_50

[566] See: United Nations, Sustainable Development Goals, Goal 3: Ensure Healthy Lives and Promote Well-Being for All at All Ages, https://sdgs.un.org/goals/goal3; and World Health Organisation, Digital Health, https://www.who.int/health-topics/digital-health#tab=tab_1

[567] European Commission (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, (COM(2020) 67 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN

[568] European Commission (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, (COM(2020) 66 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:66:FIN

[569] Ibid.

However, the most important lessons for public health and effective data sharing to support policymaking have been unravelling during the COVID-19 pandemic. The need for **coordinated measures at the EU level** quickly became clear as Member States moved to restrict the cross-border movement of people, impose lockdowns, and gradually design deconfinement policies that could still contain the spread of the virus. The lack of consistency across the data related to the pandemic limited the EU's ability to provide a coordinated and effective response at the height of the crisis in spring 2020.[570] The European Centre for Disease Control has stressed that the data on the evolution of the pandemic have several limitations, such as the fact that the **availability of public data** varies from country to country and that the **comparability of data** is dependent on the testing strategies and capacities of each Member State.[571] Transparency and common data reporting standards have thus proven to be essential for facilitating joint actions to manage public health crises in the EU.[572]

There is still significant scope for supporting data sharing and enhancing the digital health ecosystem in the EU to **strengthen public health**, deliver better health outcomes for citizens and promote well-being. To contribute to these goals, this Study provides a comprehensive overview of the **problems that negatively impact the development of digital health solutions in the EU**, mapping the regulatory barriers and market deficiencies that have so far hindered health data sharing and the creation of potential EU-wide B2B health data marketplaces, with a particular focus on Type 2 Diabetes (T2D) data and unified diabetes-related datasets. The Study relies on an extensive review of the state of the art as well as detailed input from the stakeholders in the health data ecosystem.

This analysis of **regulatory barriers and market deficiencies** is part of the wider study "Big Data and B2B platforms: the next big opportunity for Europe",[573] which aims to enhance B2B data sharing in two sectors: healthcare (with a focus on T2D) and automotive. Specific policy initiatives to address the barriers and deficiencies outlined in this document are presented in a separate report.[574] Similarly, a report on regulatory barriers and market deficiencies as well as a report detailing policy solutions were prepared for the case of B2B data sharing in the automotive field.[575]

Against this background, **this Study is structured as follows**:

[570] Renda, A., & Castro, R (2020), Towards Stronger EU Governance of Health Threats after the COVID-19 Pandemic, European Journal of Risk Regulation 11(2), pp. 1–10. Available at: https://doi.org/10.1017/err.2020.34

[571] European Centre for Disease Prevention and Control (2020), Coronavirus disease 2019 (COVID-19) in the EU/EEA and the UK – eleventh update: resurgence of cases, 10 August 2020, p. 20. Available at: https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-rapid-risk-assessment-20200810.pdf

[572] Joint European Roadmap towards lifting COVID-19 containment measures, p. 9. Available at: https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

[573] The reference for the study is: EASME/COSME/2018/004.

[574] Report on policy recommendations affecting the creation of EU-wide B2B health data marketplaces and unified diabetes-related datasets. Available as Annex XVIII of this report.

[575] Report on Recommendations to the EU and national policymakers and an action plan for the creation of shared EU-wide in-vehicle data platforms. Available as Annex IV of this report

- Section 1 *Background: The health data ecosystem* provides an overview of the key elements of the digital health ecosystem, including stakeholders and type of data;
- Section 2 *Methodology* presents the data sources and the analytical approach adopted in this Study;
- Section 3 *Market opportunities* outlines the key technological drivers that could pave the way to the development of promising services; it also explores the different governance frameworks for a potential EU-wide health data marketplace as well as the benefits that enhanced data sharing could bring to the stakeholders in the health data ecosystem;
- Section 4 *Regulatory barriers* describes obstacles related to data protection, data anonymisation and liability;
- Section 5 *Accountability and trust* details the delicate issues of transparency, responsibility for data privacy and security, as well as the challenges of building trust between the stakeholders in the ecosystem;
- Section 6 *Interoperability* emphasises the role of data standards and common frameworks to enable data sharing in the field of healthcare;
- Section 7 *Strategic barriers* lays out the potential challenges that can arise from limited access to data and emphasises the need to ensure access to data while taking into account aspects related to, among others, ethics and data protection and privacy;
- Section 8 *Other barriers* Other barrierslooks at the potential lack of qualified workforce to support the development of digital health solutions and provides an overview of the financial barriers with which SMEs are faced; and finally
- Section 9 *Policy recommendations* provides preliminary recommendations based on the identified regulatory barriers and market deficiencies.

1. Background: The health data ecosystem

The healthcare data ecosystem consists of multiple stakeholders, a variety of emerging concepts, and just as many policy issues, stemming from the fact that the field of health data is itself constantly evolving and very sensitive. This Section defines and categorises the main terms related to the healthcare data ecosystem that will be used throughout this Study.

When it comes to the **stakeholders**, public authorities, industry, academic and research institutions, and ultimately citizens are all part of the ecosystem. In particular, the following categories of stakeholders can be identified in the sub-ecosystem of T2D healthcare:

- Individuals, who can benefit from enhanced methods for health monitoring and disease prevention;
- Public authorities, including both EU institutions and national public authorities. Healthcare policy is a competence of the Member States, therefore national governments set out the policy and regulatory framework in the field. Nonetheless, the EU institutions play an important role in coordinating Member State policies , and generally the EU health policy is designed to complement national policies;[576]
- Healthcare sector, comprising pharmaceutical companies, diagnostic healthcare companies, providers of medical and hospitalisation services, manufacturers of prognostic biomarkers and biomarkers for pharmacodynamics;
- Patient associations at both national and European level, ensuring the voice of patients is heard by policymakers;
- Insurance systems, as the available prevention tools as well as disease management and treatment are crucial components of the insurance strategies that can be deployed;
- Consumer health sector, including healthcare applications (apps)/T2D platforms, personal health records facilitating companies (data intermediaries), retail/catering companies; and
- Academia and research, advancing the state of knowledge on T2D prevention and management.

Further, it is important to distinguish between the different terms that can designate the stakeholder category who is arguably the atomic source of health data: **individuals**. Depending on the context, three categories can be identified:

- Citizens or individuals – the most generic term; the use of the term 'individual' throughout this Study designates any potential data subject (that is, anyone who could share their personal data in any given context);
- Users or consumers – throughout this Study, this term designates individuals who use services, such as health apps and data intermediation services; and
- Patients – throughout this Study, this term refers to individuals in a clinical context, as recipients of medical services.

[576] Article 168 of the Treaty on the Functioning of the European Union details the framework within which the EU can adopt health legislation. See: Consolidated version of the Treaty on the Functioning of the European Union, OJ 115, 09.05.2008. See also: https://ec.europa.eu/health/policies/overview_en

The development of digital technologies means that the spectrum of the data that can be collected and shared in the field of health is expanding. Considering both traditional and newer sources of data, the following main **categories of health data** can be identified:

- Clinical (medical) data, which refer to health data collected during patient care or as part of a clinical trial. Clinical data encompasses:[577]
  - (Electronic) health records;
  - Patient/disease registries;
  - Health surveys;
  - Clinical trials data;
  - Administrative data (hospital discharge data); and
  - Insurance claims data; and
- Patient-generated health data, which differ from clinical data in that the patients are primarily responsible for capturing the data and they also determine how to distribute the data,[578] having thus a more subjective nature compared to clinical data. Patient-generated health data includes:
  - Patient-reported outcomes (data usually generated in the context of a clinical trial or in a more general clinical setting, by administering a questionnaire and receiving feedback from the patient on aspects such symptoms experienced, health status, health behaviours, quality of life);[579]
  - Biometric data;
  - Treatment history;
  - Symptoms; and
  - Lifestyle choices.

A specific subset of clinical and patient-generated health data is represented by **biomarker data**, playing an important part both in biomedical research and in a clinical setting. Biomarkers represent data stemming from any substance, structure, or process that can be measured in the body or its products and influence or predict the incidence of outcome or disease (for instance, blood pressure, body temperature, etc.).[580] Biomarkers are of particular interest as they can play an important part in the development of new therapies and drugs. There are seven main types of biomarkers, which can be divided into

[577] University of Washington Health Sciences Library (n.d.), Data Resources in the Health Sciences: Clinical Data, last updated on 23 December 2019. Available at: https://guides.lib.uw.edu/hsl/data/findclin. Last accessed: 21 May 2020.

[578] Abdolkhani, R., Gray, K., Borda, A., & DeSouza, R. (2019), Patient-generated health data management and quality challenges in remote patient monitoring, JAMIA Open, Vol. 2, Issue 4, pp. 471–478. Available at: https://doi.org/10.1093/jamiaopen/ooz036

[579] Cella, D., Hahn, E.A., Jensen, S.E., et al. (2015), Patient-Reported Outcomes in Performance Measurement, Research Triangle Park (NC): RTI Press, Types of Patient-Reported Outcomes. Available at: https://www.ncbi.nlm.nih.gov/books/NBK424381/

[580] WHO International Programme on Chemical Safety (2001), Biomarkers in Risk Assessment: Validity and Validation. Available at: http://www.inchem.org/documents/ehc/ehc/ehc222.htm. Last accessed: 21 May 2020.

two groups depending on whether they relate to the marks of a disease or the effects of drugs:[581]

- Disease-related biomarkers include: susceptibility/risk biomarkers (indicating the potential for developing a disease), diagnostic biomarkers (which confirm the presence of disease), monitoring biomarkers (used for assessing the status of a disease through serial measurement), and prognostic biomarkers (signalling the likely progression of a disease, its recurrence or the likelihood of a medical event);
- Drug-related biomarkers consist of predictive biomarkers (used to identify individuals who are more likely to show a reaction to a drug compared to similar individuals who do not have the biomarker), pharmacodynamics/response biomarkers (capturing the biological response experienced by an individual to a drug), and safety biomarkers (which are measured before and after exposure to a drug to ascertain any potential adverse effects).

Against this background, it is worth mentioning that whereas traditional biomarkers have been an integral part of research and clinical practice, a new category of indicators is emerging thanks to the digital revolution: **digital biomarkers**. Widening the spectrum of data, digital biomarkers are "physiological and behavioural measures collected by means of digital devices such as portables, wearables, implantables, or digestibles and that characterie, influence, or predict health-related outcomes."[582] Digital biomarkers fall into the wider realm of digital health. **Digital health**, as defined by the World Health Organisation (WHO), encompasses the use of ICT technology to support health and health-related fields (known as 'eHealth'), the deployment of wireless and mobile technologies in support of health objectives ('mHealth', a subcategory of eHealth), as well as new developments related to artificial intelligence (AI), big data, and genomics.[583]

The advent of digital health helps increase the **availability of real-world data**[584], including data generated by the consumers of mobile and wireless devices, leading in turn to more opportunities for **new data-based services and therapies** for patients and consumers more generally. In this sense, it is important to note that health data usage can be classified into two main categories: **primary use and secondary use**. In its primary use, health data informs the delivery of healthcare services to the individual. The **secondary use of health data** includes cases in which health data is not used for healthcare delivery, but for wider applications such as research, quality and/or safety

[581] FDA-NIH Biomarker Working Group (2006), BEST (biomarkers, endpoints and other tools) resource. Silver Spring:FDA. Available at: http://www.ncbi.nlm.nih.gov/books/NBK326791/

[582] Sim, I. (2019), Mobile Devices and Health, New England Journal of Medicine 2019, Vol. 381, pp. 956-968. Available at: https://www.nejm.org/doi/full/10.1056/NEJMra1806949

[583] World Health Organisation (2019), WHO Guideline: Recommendations on digital interventions for health system strengthening, p. 91. Available at: https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf. Last accessed: 21 May 2020.

[584] Real-world data are generally defined as data gathered outside the context of randomised controlled trials. Real-world data can include, for instance, electronic health records, registries, administrative data, health surveys, and data from mobile apps. See: Garrison Jr, L.P., Neumann, P.J., Erickson, P., Marshall, D. & Mullins, C.D. (2007), Using Real-World Data for Coverage and Payment Decisions: The ISPOR Real-World Data Task Force Report, Value in Health, Vol 10(5), pp. 326-335. Available at: https://www.sciencedirect.com/science/article/pii/S1098301510604706

measurement, public health, policy-making, development of private services, etc.[585] In the case of T2D, data (spanning from clinical data to lifestyle data) can be used for multiple purposes such as diabetes prevention, diabetes care & management and diabetes research.[586]

One of the **challenges of setting up an architecture for sharing health data** resides in the complexity of health data, their sensitive nature and who has access to and control over such data: from health records to patient-generated data, to behavioural and lifestyle data, the **means of collection** vary widely and the responsibility for the **quality of data** is also spread among multiple stakeholders based on the type of data. These considerations have implications on how **data governance** should be ensured in the field of healthcare data. Such issues are discussed at length in Sections 4 and 5.

[585] Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., Detmer, D. E., & Expert Panel (2007), Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper, Journal of the American Medical Informatics Association: JAMIA, 14(1), p. 1–9. Available at: https://doi.org/10.1197/jamia.M2273

[586] Fleming, G.A., Petrie, J.R., Bergenstal, R.M. et al. (2020), Diabetes digital app technology: benefits, challenges, and recommendations. A consensus report by the European Association for the Study of Diabetes (EASD) and the American Diabetes Association (ADA) Diabetes Technology Working Group, Diabetologia 63, pp. 229–241. Available at: https://doi.org/10.1007/s00125-019-05034-1

2. Methodology

To highlight the challenges to EU-wide B2B health data sharing, with a particular focus on T2D data, this Study relies on both desk research and in-depth interviews.

2.1 Desk research

As part of desk research, the **relevant literature** was reviewed to identify and categorise both sector-specific and more horizontal market deficiencies and regulatory barriers that are already impinging on data sharing for high-impact healthcare in the EU, or are expected to have a negative impact on the development of this field. A variety of sources was used:

- Academic literature;
- Grey literature (policy briefs, national and EU institutions reports, position papers drafted by relevant associations, etc.);
- EU legislation; and
- Policy documents accompanying EU legislation (impact assessments, ex post evaluations, interim evaluations, etc.).

The preliminary desk research revealed five main **categories of barriers and market deficiencies**:

- Regulatory barriers (including issues related to data protection, data anonymisation, and liability rules in the EU);
- Accountability and trust;
- Interoperability;
- Strategic barriers; and
- Knowledge and skills.

2.2 Fieldwork

Based on the results of the desk research, the Study Team drafted interview guidelines (in English) aiming to identify and assess market deficiencies and regulatory barriers. The guidelines summarise the **main findings of the literature review in order for these to be validated** with market players and policymakers in a structured manner.

The fieldwork activities consisted of **26 in-depth interviews** with relevant stakeholders in the digital health sector. The interviews were conducted in English either face-to-face or via phone. To ensure adequate coverage of the relevant issues, the **following categories of stakeholders** were interviewed (see Table 16 for the full overview of stakeholders):

- Academia;
- Consumer associations;
- Intermediaries/enablers of data sharing;[587]

[587] The intermediaries/enablers of data sharing represent organisations that facilitate the exchange of data in a variety of ways, such as: i) linking data subjects and data-based service providers or research organisations through an environment such as a user-centric platform; ii) collecting larger pools of data and facilitating access to the data by academia, research organisation, and/or data-based service providers; iii) helping other organisations manage and integrate data from different sources to facilitate e.g. research.

- Providers of data-based services;
- Public authorities;
- Research organisations; and
- Standardisation organisations.

Table 39 Overview of the consulted stakeholders

Organisation	Stakeholder group
Federico II University Hospital	Academia
Leiden University Medical Center (LUMC)	Academia
The European Consumer Organisation (BEUC)	Consumer association
aigora	Intermediaries/Enablers
Castor EDC	Intermediaries/Enablers
Digi.me	Intermediaries/Enablers
ELIXIR	Intermediaries/Enablers
Eurogenetica Ltd	Intermediaries/Enablers
MIDATA Cooperative	Intermediaries/Enablers
Nightingale Health	Intermediaries/Enablers
Atos	Providers of data-based services
COCIR	Providers of data-based services
European Federation of Pharmaceutical Industries and Associations, EFPIA Diabetes Platform	Providers of data-based services
Roche Diabetes Care	Providers of data-based services
Sanofi	Providers of data-based services
Health Ministry of an EU Member State[588]	Public authorities
Helsingin ja Uudenmaan sairaanhoitopiiri (HUS)	Public authorities
Kanta services, Kela (Social Insurance Institution) National Institute for Health and Welfare (THL), Finland	Public authorities
Ministry of Social Affairs, Estonia	Public authorities

[588] This stakeholder prefers to remain anonymous.

Organisation	Stakeholder group
Digital Health & Care Institute, Scotland, UK	Research organisations
EMBL-EBI	Research organisations
GO FAIR	Research organisations
INESCTEC Centre for Information Systems and Computer Graphics	Research organisations
Jožef Stefan Institute	Research organisations
National eHealth Living Lab (NeLL)	Research organisations
IEEE Standards Association	Standardisation organisations

Source: Authors' own elaboration.

The interviews were based on a **questionnaire** containing a mix of Likert-type questions,[589] and open-ended questions giving the interviewees some room for qualitative input. The Study Team computed descriptive statistics for the Likert-type questions (namely the stakeholders' answers based on a 1 to 5 scale) and compared the answers across stakeholder groups where noteworthy differences were recorded. In addition, the qualitative information provided during the interviews was aggregated, compared and summarised to support and complement quantitative indicators. Special attention was paid to **obstacles affecting SMEs**.

[589] Likert-type questions help structure the answers of respondents based on a given scale. For this Study, respondents were asked to provide their feedback on the extent to which a series of potential barriers are affecting B2B health data sharing, using a scale from '1' (not at all) to '5' (to the fullest extent).

3. Market opportunities

Understanding the market opportunities in the field of health data sharing (with a specific focus on T2D) requires a three-pronged approach: i) analysing the technological drivers that may lead to promising services in the market; ii) conceptualising a framework for the governance of a data sharing system in a way that challenges in the field are removed, opportunities are bolstered and their potential benefits are reaped in the market; and finally iii) looking at how the benefits from these new opportunities would likely be distributed among stakeholders and what this can mean in terms of incentives.

3.1 Innovation and technology driving new opportunities

Innovation in healthcare together with technological developments are opening up new market opportunities for data-driven services. Particularly in the case of T2D, new services are likely to revolve around the use of new biomarkers and personalised, science-based interventions, which can hold significant potential in the context of **EU-wide B2B health data marketplaces** and unified datasets for diabetes data.

The discovery of **new biomarkers** (both disease-related and drug-related biomarkers) could represent potential opportunities in the field of T2D, in a variety of ways:

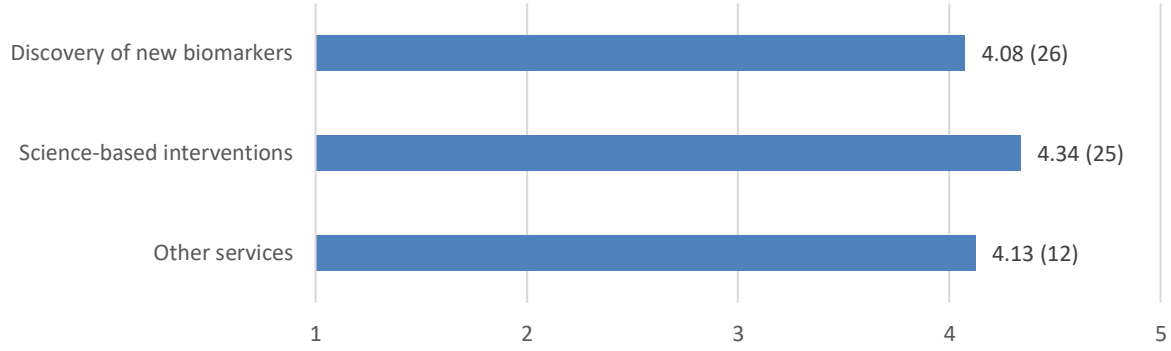
- Susceptibility biomarkers that help evaluate the risk of developing T2D and may offer opportunities for preventive action;
- Diagnostic biomarkers that are used to monitor the health status and may offer opportunities for preventive action;
- Biomarkers to predict whether a treatment will be more successful for a certain group of patients;
- Prognostic biomarkers that help create health trajectories for T2D patients; and
- Biomarkers for pharmacodynamics that are able to quantify the dose-effect relationship in a particular time course of T2D medication.

Additional market opportunities are represented by **science-based and personalised interventions**. These interventions, which rely on newer indicators such as digital biomarkers and wider behavioural and lifestyle data about individuals, could be medically-driven (for instance, targeted drug treatments) as well as lifestyle-based, such as nutritional and lifestyle advice models.

For T2D, therefore, new data and services represent significant potential opportunities in the market, considering that the **management of the disease** is rather complex, with multiple factors affecting the well-being of patients.[590] The stakeholders consulted for this Study confirm almost across the board that new biomarkers and emerging science-based interventions represent **promising market opportunities** for EU-wide B2B health data marketplaces (see Figure 69). This takeaway is also reflected by the emerging research in the field.

[590] Fagherazzi, G., & Ravaud, P. (2018), Digital diabetes: Perspectives for diabetes prevention, management and research, Diabetes & Metabolism, Vol. 45:4, pp. 322-329. Available at: https://doi.org/10.1016/j.diabet.2018.08.012

Figure 69 Extent to which data-based healthcare services may represent promising market opportunities for the EU industry and SMEs in the field of T2D (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

By way of example, **susceptibility biomarkers** can support proactive therapies for individuals at risk of developing the condition. The International Diabetes Federation estimates that there are currently over 370 million adults aged 20 to 79 affected by prediabetes (corresponding to 7.5% of the population in this respective age group) and this number is predicted to reach almost 550 million by 2045 (8.6%).[591] Thus, the **asymptomatic period before the full onset of the disease** can be seen as an opportunity to prevent or modulate the development of the disease. The discovery of additional biomarkers and new ways of combining them can result in a better, more sensitive, and more specific prediction of the likelihood of developing diabetes and provide better opportunities for preventive action.[592] **Proactive therapies** can include primary preventive actions, such as interventions designed to correct unhealthy behaviours and to help patients avoid risk factors, as well as secondary preventive actions, meant to slow down the progression of the disease.[593]

In a similar fashion, for patients diagnosed with T2D, new biomarkers can help develop **better treatments and better targeting of treatments**, thus improving disease management. Combinations of potential genetic, behavioural and environmental biomarkers can help improve how T2D patients are categorised in sub-groups, facilitating a **precision-medicine approach**.[594] In developing more targeted drug treatments, technological developments such as **AI and machine learning** could play an important

[591] International Diabetes Federation (2019), IDF Diabetes Atlas, 9th ed., Brussels, Belgium: International Diabetes Federation, p. 35. Available at: https://www.diabetesatlas.org/en/

[592] Dorcely, B., Katz, K., Jagannathan, R., Chiang, S. S., Oluwadare, B., Goldberg, I. J., & Bergman, M. (2017), Novel biomarkers for prediabetes, diabetes, and associated complications. Diabetes, metabolic syndrome and obesity: targets and therapy, Vol. 10, pp. 345–361. Available at: https://doi.org/10.2147/DMSO.S100074

[593] Gedela, S., Appa Rao, A., & Medicherla, N. R. (2007), Identification of biomarkers for type 2 diabetes and its complications: a bioinformatic approach, International journal of biomedical science: IJBS, Vol. 3(4), pp. 229–236. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3614656/

[594] Laakso, M. (2019), Biomarkers for type 2 diabetes, Molecular Metabolism, Vol. 27, Supplement, pp. S139-S146. Available at: https://doi.org/10.1016/j.molmet.2019.06.016

role in bringing together a large variety of data – clinical data, biological profile, lifestyle data – and develop novel insights for therapies modelled for sub-groups of patients that share specific characteristics.[595]

Science-based and personalised interventions seem to be relatively more promising for market services though. One reason is that biomarkers, while crucial drivers of developments in the field, take a relatively long time to be adopted into practice. The process involves the discovery of biomarkers, experiments, clinical studies, and analytical validations among other steps, all requiring the involvement of multiple stakeholders, from academia and medical professionals to industry and regulatory authorities.[596] As such, science-based interventions, powered by digital biomarkers, are seen as more promising given that they measure aspects that are not strictly related to the health status of a person but also account, more generally, for one's well-being.

When it comes to **lifestyle interventions**, patient-generated health data can be significantly enhanced through the use of different technologies, such as smartphone apps and connected devices more generally, to **improve disease management** and lifestyle. Digital biomarkers and patient-generated health data provide the means for healthcare programmes specifically targeted to the individual patient, such as personalised nutrition plans adapted to the glycaemic and microbiota profile of the patient.[597] The advantages of these new developments consist in the ability to **deliver real-time care** and **collect remotely more and better data about a patient's health status**.[598]

Other developments could represent promising market opportunities, as emphasised by the consulted stakeholders and reflected by emerging research. What appears to be particularly interesting is **the universe surrounding healthcare and well-being programmes**.

- **Digital health apps**. Apps offering lifestyle advice based on consumer data are gaining in popularity, and that is the case particularly for weight management apps. A systematic review of the efficacy of mobile phone apps for lifestyle interventions, which was published in 2019, shows that apps are useful tools for supporting lifestyle modifications in patients with T2D.[599] Such **lifestyle apps** can include a variety of functions, including lifestyle monitoring, health education, medication adjustment, recording different measurements, and feedback based on the data tracked. The take-up of digital health apps may still depend significantly on the

[595] Seyhan, A.A., & Carini, C. (2019), Are innovation and new technologies in precision medicine paving a new era in patients centric care?, Journal of Translational Medicine, Vol. 17: 114. Available at: https://doi.org/10.1186/s12967-019-1864-9

[596] Babrak, L. M., Menetski, J., Rebhan, M., Nisato, G., Zinggeler, M., Brasier, N., Baerenfaller, K., Brenzikofer, T., Baltzer, L., Vogler, C., Gschwind, L., Schneider, C., Streiff, F., Groenen, P. M. A. & Miho, E. (2019), Traditional and Digital Biomarkers: Two Worlds Apart?, Digit Biomark 2019, Vol. 3, pp. 92-102. Available at: https://doi.org/10.1159/000502000

[597] See note 590.

[598] See note 595.

[599] Wu, X., Guo, X., & Zhang, Z. (2019), The Efficacy of Mobile Phone Apps for Lifestyle Modification in Diabetes: Systematic Review and Meta-Analysis, JMIR mHealth and uHealth, Vol. 7(1). Available at: https://doi.org/10.2196/12297

advice given by healthcare professionals to purchase such apps and on whether the costs are reimbursed by health insurance schemes.[600]

- **Digital advice**. An additional functionality, that may be welcome in the market, consists of digital health apps that provide **chatbox-like interactions**, resembling telemedicine but offering lifestyle advice instead of pure medical advice that only a medical practitioner can give. Such interventions are already being rolled out as trials. For instance, in the UK, Nestlé, together with Tesco, implemented in 2019 a wide-scale nutritional intervention programme targeting specifically T2D patients. The intervention is a clinically-supported weight-management programme ('OptiJourney') in which participants follow a low-calorie diet and can receive support from dietitians and coaches via an app, as well as from a local pharmacist.[601]
- **Quality control**. With new therapies emerging, another potential opportunity in the market is represented by research studies providing evidence of therapy effectiveness and safety, especially in the case of digital health apps. Traditional studies on the effectiveness of interventions include complex, long-duration investigations such as randomised controlled trials and cohort studies, whereas digital health apps tend to be quite fluid, changing over time and having a shorter lifespan compared to traditional, purely medical interventions.[602] Therefore, there can be a market opportunity for developing a quality assurance mechanism better tailored to the nature of digital interventions, for instance through **services that test digital health apps and provide an evaluation of their claims and results**.[603]
- **Research**. In addition, new technologies and big data may enable more opportunities for the **secondary use of health-related data**. Open data models are promising frameworks to enable access to data and allow for the possibility to harness different data into research and precision medicine. For instance, data lakes can enhance research by facilitating access to large pools of data.[604]
- **Awareness**. Finally, another potential market opportunity revolves around services designed to increase awareness about the consequences of chronic

[600] Market analysis of the potential of European B2B platforms and unified European diabetes-related data sets. Available as Annex VI in this report.

[601] See: https://www.nestlehealthscience.co.uk/myoptijourney/programme

[602] See note 586, p. 241.

[603] An example of such a testing service could be an eHealth app rating tool, assessing apps on several dimensions such as their quality and safety, as well as the relevance and value brought to users and practitioners. See Levine, D.M., Co, Z., Newmark, L.P. Groisser, A.R., Holmgren, A.J., Haas, J.S. & Bates, D.W. (2020), Design and testing of a mobile health application rating tool, Npj Digital Medicine, Vol. 3(74). Available at: https://www.nature.com/articles/s41746-020-0268-9

[604] A data lake is a system of data stored in its raw format that help pool together data from different sources in a quick but unstructured way, shifting the data curation and integration processes onto those who access the data. See, for instance: Grossman, R.L. (2019), Data Lakes, Clouds, and Commons: A Review of Platforms for Analyzing and Sharing Genomic Data, Trends in Genetics, Vol. 35(3), pp. 223–224. Available at https://doi.org/10.1016/j.tig.2018.12.006

diseases like T2D. Such services would be instrumental especially for prevention and early diagnosis.

3.2 Ownership models

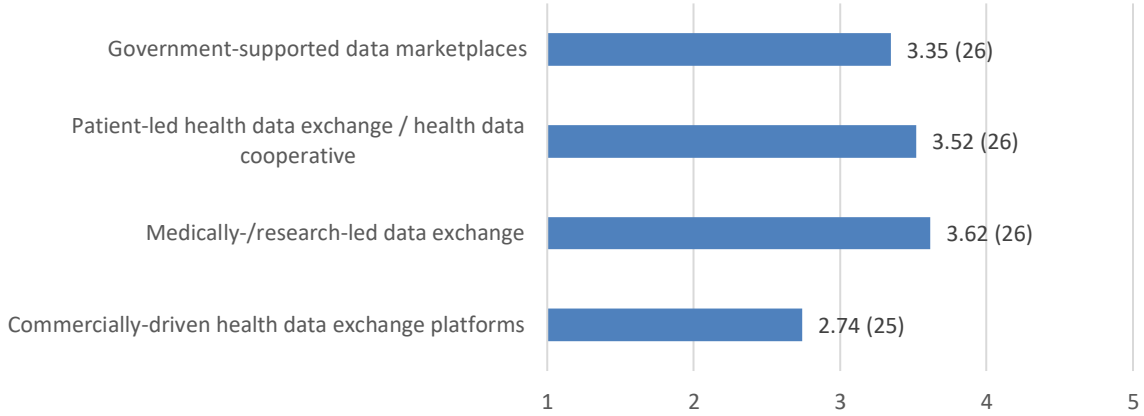
EU-wide B2B health data marketplaces and unified diabetes-related datasets may rely on different ownership models. With various opportunities in the market for new data-driven services, the question is what kind of framework could best support the provision of such services and could lead to the creation of market opportunities for the EU industry and SMEs. Based on the classification of the main stakeholders in the field, as laid out in Section 1, four main types of ownership models can be defined:[605]

1. **Government-supported data marketplaces**, in which public authorities would take the leading role;
2. **Patient-led health data exchanges and health data cooperatives,** which would be based on patient empowerment and would place the patient, and more generally individuals, at the heart of data sharing;
3. **Medically- and research-led data exchanges**, in which research organisations and hospitals would define and support the data-sharing framework, channelling the vital role of data for research; and finally
4. **Commercially driven health data exchange platforms**, in which businesses would take the leading role in providing the services that enable data sharing.

The ownership model plays an important part in developing a trustworthy data-sharing system and engaging multiple stakeholders. The feedback from the stakeholders interviewed for this Study reflects the mix of advantages and disadvantages stemming from each ownership model (see Figure 70).

[605] See also: Market analysis of the potential of European B2B platforms and unified European diabetes-related data sets. Available as Annex VI in this report.

Figure 70 Extent to which different ownership models may favour the provision of data-based health services related to T2D and create market opportunities for the EU industry and SMEs (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

Given the prevalence of some level of universal public health in the EU Member States, a **government-supported model** could be advantageous as public authorities are already a prominent stakeholder in the provision of healthcare services. Such a model may be more likely to get more people on board and instil trust in the data sharing process by relying on a comprehensive regulatory framework and oversight mechanisms. At the same time, the progress in the field may be slow and subject to budgetary constraints and political priorities.

A **patient-led model** is centred on the fact that the patient is the ultimate, atomic source of data, whether it is biometric, behavioural or lifestyle data. In this regard, single-source data, meaning all data collected from a single individual, is a powerful data type, allowing for targeted interventions and novel insights to be drawn, as emphasised during the interviews. The widespread use of smartphones can be a catalyst for enabling wider patient participation. Additionally, in a patient-led model, patient associations can play a central role, not only to mobilise patients but also when it comes to the unique data that they hold, such as experiences shared by patients about therapies or outcomes of specific actions. This model could hold great promise for medical research (unlocking a wider pool of data) and for patients (by harnessing their data into targeted interventions). At the same time, however, there are certain drawbacks to the model. Even in the presence of patient associations, **mobilising patients** to such an extent that they lead the development of a health data sharing marketplace is a very difficult task. Such mobilisation can be seen in patients with rare, life-threatening conditions, but may be rather hard to achieve for a disease like T2D that may not be seen as immediately life-threatening. A patient-led model can be facilitated by **intermediaries** who link patients and their data to academia, research organisations, or providers of data-based services. The stakeholders consulted for this Study emphasised that new technologies, such as **distributed-ledger technologies**, can support a patient-centric, or more broadly a

user-centric model, as they prevent the data from being tampered with and ensure enhanced data security.[606]

A **medically- or research-led model** tends to be the most preferred option, from the point of view of the consulted stakeholders, when analysing the different models and discounting potential hybrid systems. A medically- or research-led model can instil more trust than other models through the structure, procedures, and oversight embedded in research and thus convince more individuals to engage in the data-sharing system. Such a model is, however, still very close to a government-led approach, considering that **medical and research activities in most EU countries are carried out in great part by public institutions**, i.e. public universities and hospitals. Potential drawbacks of such a model would include conflicted interests between researchers, for whom exclusive access to data would be desirable for research purposes, and patients, who may wish to share their data widely, as necessary, to gain access to the needed or desired services. Limiting access to data by other stakeholders may also restrict innovation, considering that the field is also driven by commercial stakeholders.

Finally, a **commercially driven model** would seem to have more drawbacks than advantages. While commercial initiatives can drive innovation by mobilising significant financial resources and delivering results relatively fast, such a model would have a rather significant **trust issue**, casting questions about monetising data.

Naturally, given the complexity of the field and the pros and cons discussed above, there is **no perfect ownership model** for EU-wide B2B health data marketplaces and unified diabetes-related datasets. Rather, the best model to support developments in the field could be a hybrid one, as also indicated by the consulted stakeholders. Based on the advantages and disadvantages of each individual model and on the feedback from stakeholders, several configurations of a hybrid model could be envisioned:

- A **patient-medical hybrid model** would bring together the main categories of data (clinical and patient-generated) and channel them into improved therapies. Trust in the model and sense of ownership would be high thanks to the engagement of patients as well the reputation of the medical sector;
- A **commercially-driven model combined with a patient-centric approach** could spur innovation, by ensuring a dynamic process for developing data-based services, with the patient being in control of sharing their data. In addition, research activities could enhance this model by helping validate outcomes and thus instil more credibility in the approach; and
- A **fully mixed model**, with patient, medical, commercial and governmental data that are interoperable, would bring significant value, as the value of data nowadays is substantially enhanced when looking beyond single datasets or silos.

For any configuration of ownership models, a **trustworthy framework with clear rules and transparency** is essential to engage as many stakeholders as possible from different

[606] Saha, A., Amin, R., Kunal, S., Vollala, S. & Dwivedi, S.K. (2019), Review on "Blockchain technology based medical healthcare system with privacy issues", Security and Privacy, Vol: 2:e83. Available at: https://doi.org/10.1002/spy2.83

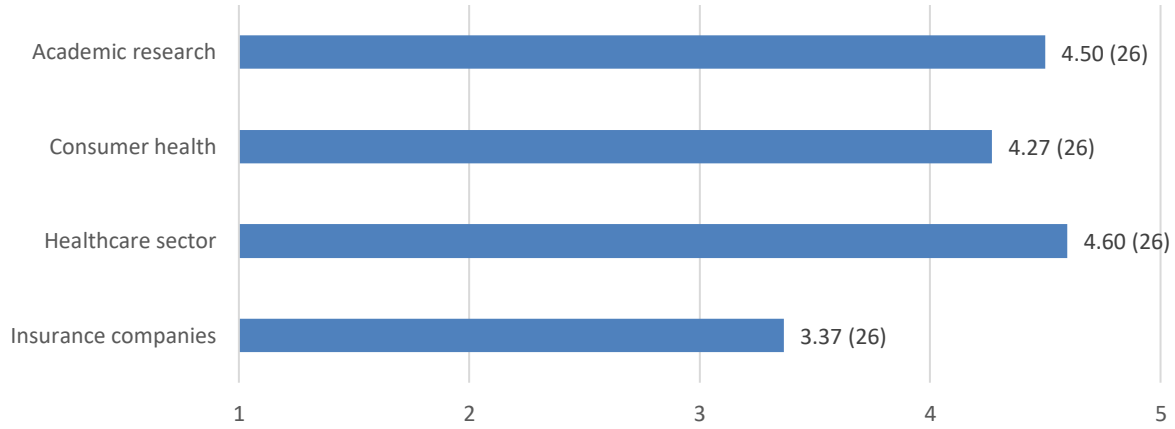
stakeholder groups.[607] This can mean, for instance, that there is scope for **governmental guidelines and oversight in the field**, along with adherence to **relevant standards**. To ensure an EU-wide marketplace for data sharing, the role of public authorities (both EU and national) is crucial for coordination purposes. Otherwise, different solutions devised nationally by different stakeholder groups may result in a fragmented landscape.

The discussion on **ownership models** as presented in this Section highlights which stakeholders could play a leading role in the development of EU-wide health data marketplaces and why. This overview is essential to understand the **different perspectives brought by the variety of stakeholders** in the health data ecosystem and the main drivers behind their support for certain models. Irrespective of the model, regulatory barriers and market deficiencies impinging on data sharing will need to be addressed (the regulatory barriers and market deficiencies are detailed in Sections 4 to 8) to allow the market to develop and eventually move towards an ownership structure accepted and supported by stakeholders.

3.3 Benefits

As feedback from the consulted stakeholders confirms (see Figure 71), an EU-wide B2B health data marketplace could **provide benefits across the board**, to different market segments. Some caveats are, nonetheless, attached to the identified potential benefits.

Figure 71 Extent to which different market segments may benefit from EU-wide B2B health data marketplaces and unified diabetes-related datasets (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

The **healthcare system** already produces a significant amount of data. Through an enhanced framework for data sharing, the system could better exploit the existing data, drawing more insights from them and having the potential to deliver improved services.

Owing to new technologies that facilitate the development of data-based services, the **consumer health sector** would see its growth further increased by an enhanced data-

[607] COCIR (2019), European Health Data Space: Towards A Better Patient Outcome. Available at: https://www.cocir.org/media-centre/publications/article/european-health-data-space-towards-a-better-patient-outcome.html. Last accessed: 21 May 2020.

sharing framework, especially since the services falling into this category vary from health monitoring to nutrition and lifestyle advice.

For **insurance companies**, additional data may allow them to provide the best health plan for insured individuals. However, stakeholders emphasised that there should be a legal framework in place to **prevent undesired outcomes such as the refusal of coverage**. In this sense, the **right to be forgotten** plays an important part to prevent that certain diseases have a negative impact on how insurance companies perceive risks associated with a patient. It should be noted, however, that the role of insurance companies in the market varies from country to country, especially between private and public healthcare systems.

Finally, **academic research** is also very likely to benefit from an EU-wide B2B health data marketplace, as increased availability of data and new data sources can pave the way to innovative research. In the same vein, clinical trials could be further supported by these new developments.

4. Regulatory barriers

This Section analyses barriers around data protection in the EU, questions of data anonymisation, as well as liability and responsibility for data quality, identifying actual and potential regulatory barriers that may impede the development of B2B health data marketplaces and unified diabetes-related datasets.

4.1 Data protection in the EU

Sensitive data, consent, and sanctions in the framework of the GDPR

The General Data Protection Regulation (GDPR)[608] has provided a **comprehensive framework for data protection and privacy**[609] in the EU. When it comes to the potential of a health data marketplace, this Regulation is pivotal in any technical framework that would facilitate data sharing. In particular, the GDRP is relevant through its provisions on consent, sanctions in case of non-compliance, special requirements for sensitive data (as a specific category within personal data), as well as data portability, which have an impact on the incentives of different stakeholders to share data and to develop data-based services. In addition, the way the GDPR is implemented in the Member States and any additional national measures for data protection, whether more general or specific to the field of health, also need to be considered.

The rules set out by the GDPR concerning the **consent of data subjects** (as outlined in Article 7) require the appropriate infrastructure to be put into place for the processing of data (for which the general conditions are outlined in Article 6 of the GDPR). In particular, the consent of data subjects must be requested in a clear and intelligible form, distinguishable from other matters, and the consent given should reflect the "freely given, specific, informed and unambiguous indication of the data subject's agreement".[610] In addition, data subjects have the right to withdraw their consent just as easily as it was for them to give it in the first place.[611]

Importantly, **the data subject has specific rights** that need to be considered in certain cases of health data processing. These rights include:

- The right of access (Article 15 of the GDPR);
- The right of rectification of inaccurate or incomplete personal data (Article 16 of the GDPR);

[608] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[609] Together with the GDPR, the ePrivacy Directive (Directive 2009/136/EC) contributes to protecting the digital privacy of EU citizens. The Directive, adopted in 2002 and amended in 2009, sets out rules for the confidentiality of communications as well as for online monitoring and tracking. In 2017, the Commission put forward a proposal for a Regulation on Privacy and Electronic Communications, to adapt the Directive to the GDPR and respond to new challenges brought by technological developments. The proposal has not yet been adopted and is currently discussed in the Council. See: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[610] See GDPR, Recital 32 and Article 7 (see note 608).

[611] Ibid, GDPR, Article 7.

- The right to be forgotten (to demand personal data be erased by the data controller) (Article 17 of the GDPR);
- The right to restriction of processing (Article 18 of the GDPR);
- The right to data portability (Article 20 of the GDPR); and
- The right to object to the processing of personal data (Article 21 of the GDPR).

In addition, Article 5 of the GDPR outlines the **key principles for processing personal data**, essentially the backbone of the data protection framework: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

The GDPR differentiates between personal data and **sensitive data**, with stricter requirements applying to the latter category (Article 9 of the GDPR).[612] Data concerning health is classified under GDPR as sensitive data and defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".[613] In addition to data concerning health, the GDPR also covers genetic and biometric data. This distinction between personal data and sensitive data is particularly relevant for mobile health (mHealth) solutions, which must comply with stricter rules when gathering health or biometric data in comparison to personal data only. The GDPR thus provides a legal basis for the data subjects (for instance, patients) to decide whether to share data such as digital biomarkers generated through the use of health apps, and for the data controllers to transfer the data to other parties.

In this context, **processing of health data** is jointly governed by Article 9 and Article 6 of the GDPR, outlining the general framework for data processing. Based on the provisions related to sensitive data, the processing of health data is generally prohibited, unless the data subject provides his/her **"explicit consent" for one or more specific purposes** (according to Article 9 (2) lit. (a) of the GDPR). In other words, transparency is essential: the data subject must be fully aware of the purpose of the data processing and health data must not be disclosed to third parties without the permission of the data subject. At the same time, Article 9 envisages a number of **cases in which the processing of sensitive data can take place without the explicit consent** of the data subject. With relation to health data, the following purposes are particularly relevant:

- To protect the "vital interests" of a person, when that person is not able to provide explicit consent (Article 9 (2) lit. (h) of the GDPR);
- To protect "public interest in the area of public health", which includes "ensuring high standards of quality and safety of health care and of medicinal products or medical devices", provided that "suitable and specific measures to safeguard the rights and freedoms of the data subject" are in place (Article 9 (2) lit. (i) of the GDPR);
- To conduct scientific research, provided that "suitable and specific measures to safeguard the rights and freedoms of the data subject" are in place (Article 9 (2) lit. (j) of the GDPR); and

[612] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.

[613] See GDPR, Article 4 (see note 608).

- If the data is already made publicly available by the data subject (Article 9 (2) lit. (e) of the GDPR).

In light of the provisions of the GDPR, there are multiple ways in which new technologies based on health data can be deployed. For instance, targeted, **personalised health services** can be implemented by requesting the "explicit consent" of a patient or, more generally, the explicit consent of the user of the health service. **Solutions based on big data** could be implemented to improve the way medicines or medical devices function, with the GDPR allowing the processing of health data in this context as long as the safeguards exist and the rights of the patients or users providing the data are respected. **Scientific research** can also benefit from the framework of the GDPR, provided that safeguards are in place and the principle of data minimisation is respected, i.e. using only the necessary data for the purposes of the research, including by applying **de-identification techniques** if this does not have any impact on the purposes of research (Article 89 of the GDPR). In addition, in the context of research, the GDPR also allows for derogations from the right of access, right of rectification, right of restriction of processing, and right to object to the processing of personal data (Article 89(2)). It is noteworthy, however, that the right to be forgotten still holds. This implies that the crafting of studies must be done in such a way as to allow for data to be erased at the request of the data subject.

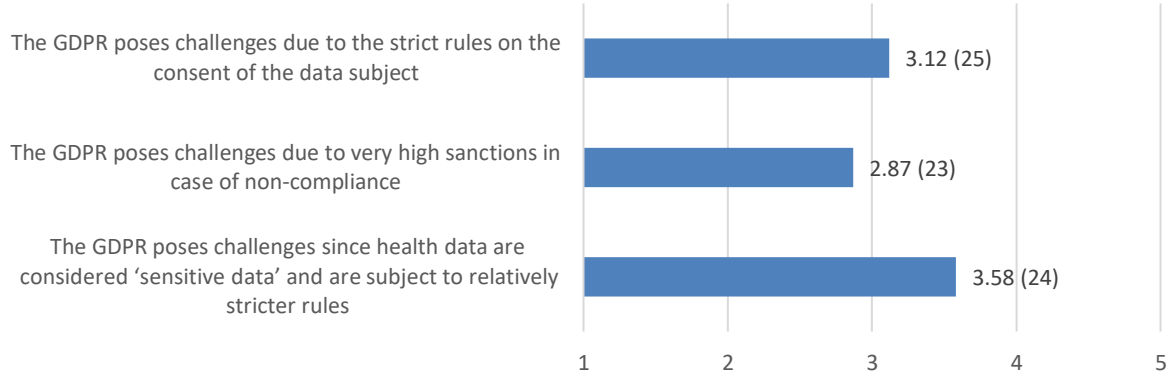
Finally, the GDPR sets out significant **sanctions in case of non-compliance** with personal data privacy legislation, compared to the previous Directive on data protection.[614] Article 83 of the GDPR sets out an administrative fine of "up to 20,000,000 euros, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher" when there is an infringement of personal data rights. This provision can trigger **expensive lawsuits and fines** for breaking the rules on principles for data processing, including conditions for consent, the data subjects' rights and the transfers of personal data to a third party.

Against this backdrop, the stakeholders consulted for this Study see both **obstacles and advantages in the rules set out by the GDPR**. On average, the stakeholders confirm that the GDPR, through its requirements on the consent, the provisions on sensitive data, and the risk of sanctions, poses some challenges (see Figure 72), as it requires a **rigorous consent architecture** be put in place, both for personal data and sensitive data. Importantly, these issues are **considered especially challenging by SMEs** compared to other entities in the field, according to the consulted stakeholders. The risk of sanctions is in particular emphasised as a burden for SMEs, who consider this risk to be challenging to a high extent.

At the same time, however, the GDPR is also seen as an **enabler for data sharing**. Its requirements can in fact contribute to **increasing trust** and thus support the development of data sharing architectures. Moreover, the threat of sanctions is actually seen as even less of an impediment compared to the requirements for consent or those for sensitive data. The threat of sanctions is considered necessary by stakeholders to build more trust in the system and ensure compliance, particularly in a field like healthcare where trust is essential (see also Section 5 for an in-depth discussion on the role of trust and accountability).

[614] Hoofnagle, C.J., Van der Sloot, B. & Zuiderveen Borgesius, F. (2019), The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, Vol. 28(1), pp. 65-98. Available at: https://doi.org/10.1080/13600834.2019.1573501

Figure 72 Challenges posed by the GDPR to the creation of B2B health data marketplaces and unified diabetes-related datasets in the EU (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

Several sanctions have already been applied for data breaches or mishandling of health data and patient data. Stakeholders affected include business and public institutions alike.[615] For example, one of the most recent cases involved breaches of the GDPR in a hospital in Rhineland-Palatinate, Germany, as a result of patient data mix-up upon admission of a patient. The Commissioner for Data Protection and the Freedom of Information of Rhineland-Palatinate noted the importance of health data protection, emphasising that such corrective measures should be taken as a signal "that the data protection supervisory authorities are particularly vigilant in the field of data handling in health care."[616]

A 2019 study[617] provides initial evidence for the challenges and adjustment costs stemming from the GDPR. Based on an EU-wide analysis of the financial performance of hospitals before and after the adoption of the GDPR in 2016, the study shows that hospitals that have a significant digital health component have suffered from **financial distress after the adoption of the GDPR**, suggesting that hospitals incurred adjustment costs to prepare for the coming into force of the Regulation. Such adjustment costs could include, for instance, the training of staff or recruitment of new staff, redesigning processes, upgrading technical equipment, etc. The paper also shows initial evidence of the **effectiveness of the GDPR** – hospitals with digital services took measures to adapt and comply with the new data protection framework.

The insights drawn from the experience of hospitals could have wider implications, considering that such **adjustment costs** may be incurred also by other stakeholders in

[615] An overview of sanctions applied for breaches of the GDPR can be found at: https://www.enforcementtracker.com/

[616] EDPB (2019), Fine against hospital due to data protection deficits in patient management, last updated on 3 December 2019. Available at: https://edpb.europa.eu/news/national-news/2019/fine-against-hospital-due-data-protection-deficits-patient-management_en. Last accessed: 21 May 2020.

[617] Yuan, B. & Li, J. (2019), The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation, International Journal of Environmental Research and Public Health, Vol: 16(6). Available at: https://doi.org/10.3390/ijerph16061070

the market, such as providers of services based on data. In particular, such costs may pose more **challenges for SMEs**, who might find it more difficult to adjust to the requirements. At the same time, however, feedback from the interviews also shows that relevant stakeholders have been generally aware of the importance of data protection in the field of healthcare and some businesses implemented safeguards for data protection even before the adoption of the GDPR. The feedback in this regard reinforces the general idea that trust is essential. The **GDPR contributes to ensuring a trustworthy framework**, but some stakeholders may also take measures themselves to gain the trust of data subjects, without being mandated to do so by legislation.

Box 3 COVID-19: Data protection in times of pandemic

In the first half of 2020, the global outbreak of COVID-19 not only brought the EU economy to a standstill as lockdown measures were introduced in the Member States, but it also put a spotlight on data protection and privacy when handling sensitive personal data. Importantly, the ensuing discussions sparked by the pandemic can reverberate beyond the containment of COVID-19. When taking stock of the experience of the pandemic from a data protection point of view, there are two key items to consider: i) the legal basis for collecting and using personal data in the midst of a public health crisis must be clear; and ii) any measures to tackle the crisis must be taken with careful consideration of any future implications, to avoid backlash from citizens if the question of data protection is not treated carefully.

What is the legal basis for collecting and using personal and health data during the crisis?

The GDPR provides a framework for the processing of personal and health data based on the explicit consent of the data subject, as laid out in Articles 6 and 9. The GDPR also allows for derogations from the obligation to obtain the explicit consent of the data subject to process health data in special circumstances, including for managing "cross-border threats to health", as detailed in Article 9(2) lit. (i) of the GDPR. In addition, Article 9(2) lit. (j) of the GDPR provides the legal basis for the processing of health data for the purpose of scientific research. The European Data Protection Board (EDPB) has also issued specific guidance on the processing of health data for scientific purposes,[618] outlining Articles 5, 6 and 9 of the GDPR as the main legal basis.

Data protection in such a sensitive context plays a paramount role for gaining the trust of citizens, as the EDPB also emphasised in a statement issued on 19 March 2020.[619] To this end, respecting the core principles of the GDPR (including transparency, lawfulness, and accountability) is crucial. The GDPR, however, is only one aspect of the legal basis for processing data in the context of the COVID-19 outbreak. The use of contact tracing apps in the context of the crisis, which has essentially represented the core of the debate on data privacy and protection, also triggers the provisions of the ePrivacy Directive with regards to the use of location data. According to specific guidelines from the

[618] EDPB (2020), Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 April 2020. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

[619] EDPB (2020), Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

EPDB,[620] Articles 5, 6 and 9 of the ePrivacy Directive allow for the collection of data directly from the user's device and for the transmission of anonymised data from electronic communication providers to public authorities or third parties.

The GDPR and the ePrivacy Directive have provided the legal basis for introducing contact tracing apps, but some Member States also considered it necessary to adopt additional legislation at the national level to facilitate the launch of such apps (for instance, Italy, Finland, and Estonia).[621] Even though this is an example of a swift intervention as part of the COVID-19 crisis management, it does point to the fact that, while the GDPR and the ePrivacy Directive provide a horizontal framework for data protection and privacy, sector-specific measures may well be considered and adopted by Member States if deemed necessary by national authorities. In this case, the key is to ensure coherence with EU rules and coordination of national rules.

Looking forward: Will citizens be more or less willing to share data and adopt data-driven services?

Striking the right balance between creating effective tools to combat the spread of the virus and ensuring the privacy and protection of data is the main challenge both for the short- and long-term. In the short-term, data-driven tools could help contain the virus. In the long-term, the impact of measures taken during the crisis may impact trust in data sharing, if perceived as too intrusive into one's privacy.[622]

Self-diagnosis apps and contact tracing apps have shed a different light on the technology that most citizens use on a daily basis, emphasising its potential beyond established purposes. This experience can be exploited as the starting point for showing to citizens the potential of data collected through everyday devices for improving the provision of healthcare services. On a broader policy level, the crisis could also give more momentum to health data initiatives and to the European Health Data Space, by drawing lessons from the COVID-19 experience and focusing on enhanced cooperation between Member States. Nevertheless, such technology-based measures could backfire and citizens may be less willing than before to engage with them and share data if privacy concerns go unmitigated. As society transitions to a new normal (until a vaccine becomes available), privacy will need to be carefully balanced with the efforts to contain the virus to secure the trust of individuals.

The role of data portability

One of the central features of the GDPR, which led the consulted stakeholders to describe the Regulation as an enabler for user-centric data sharing, is the provision related to data

[620] EDPB (2020). Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[621] European Commission (2020), Mobile applications to support contact tracing in the EU's fight against COVID-19, Progress reporting, June 2020. Available at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf

[622] See: Renda, A. (2020), Will privacy be one of the victims of COVID-19?, published on 23 March 2020, CEPS In Brief. Available at: https://www.ceps.eu/will-privacy-be-one-of-the-victims-of-covid-19/

portability. Some authors would go as far as to describe data portability as "the first theoretical step towards a **default ownership of personal data to data subjects**".[623]

Article 20 of the GDPR gives individuals the right to request and receive their personal data that is in the possession of a data controller "in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller".[624] With this provision, the GDPR puts the individual in the unique position of being able to **aggregate valuable data along multiple dimensions** (health, shopping, fitness, etc.), with novel opportunities for developing 'single-individual' datasets that could play an important role in personalised healthcare and well-being services.

Importantly, the right to data portability is also a way of **increasing competition among 'data collectors'**.[625] When data subjects can gain access to their personal data and decide with whom they wish to share the data, this area will no longer be monopolised but open to new market opportunities. While the opportunity is available, taking action may not be as simple. In the end, how easy is it for individuals to track all their data, scan opportunities for novel data-based services, and decide with whom to share the data? Taking this into account, data portability can also lead to the creation of **new services that facilitate the way individuals tap into the potential of their data** and share them with service providers of their choice. Such services include intermediaries facilitating data exchanges between individuals, businesses and data cooperatives (see Section 0 for further details).

The right to data portability could be bolstered by including more **technical specifications that facilitate interoperability**. Article 20 currently specifies that personal data should be made available in a machine-readable format. However, such a format does not immediately guarantee ease of access and ease of transfer. For this reason, some stakeholders in the field suggest amending this provision to specify more clearly that **access should be made available through application programming interfaces** (APIs).[626]

Other rules on personal and health data protection

Beyond the GDPR, additional EU rules as well as national rules related to personal and health data complete the picture of data protection. For example, the **Cross-border Healthcare Directive** (2011/24/EU)[627] recognises the protection of personal health data (as a shared responsibility of the Member State of affiliation and the Member State of

[623] De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L. & Sanchez, I. (2018), The right to data portability in the GDPR: Towards user-centric interoperability of digital services, Computer Law & Security Review, Vol. 34(2), pp. 193-203. Available at: https://doi.org/10.1016/j.clsr.2017.10.003

[624] GDPR, Article 20 (see note 608).

[625] Hafen, E. (2019), Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health, in: Krutzinna J. & Floridi L. (eds), The Ethics of Medical Data Donation, Philosophical Studies Series, Vol. 137, Springer, p. 143. Available at: https://link.springer.com/chapter/10.1007%2F978-3-030-04363-6_9

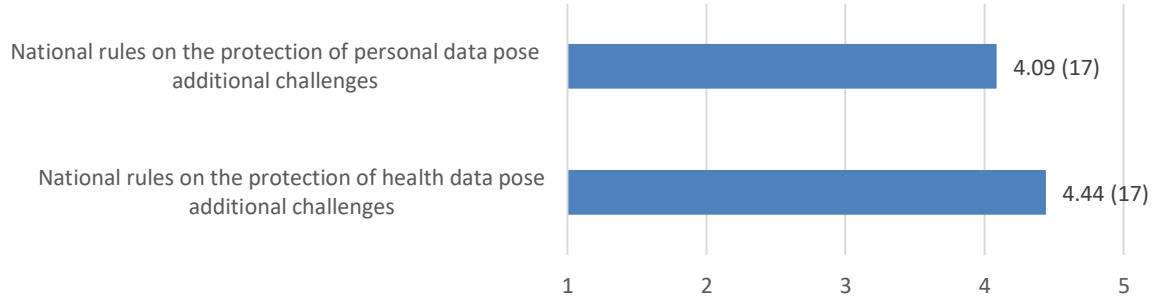
[626] See: Cozy Cloud, MyData Journal, "We want our data back using APIs!", in Medium, published on 2 March 2017. Available at: https://medium.com/mydata/we-want-our-data-back-using-apis-799646412ff2

[627] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, pp. 45–65. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0024

treatment) and includes rules on the safe transmission of personal health data, as one of the essential preconditions for ensuring continuity of healthcare across borders.

Differences between Member States can appear in terms of the regulatory framework applicable to health data protection, as the GDPR allows for **additional measures to be taken at the national level** as deemed necessary by each country. In addition, health policy is a field that is regulated at the national level, with the EU playing only a coordinating role, as the consulted stakeholders also indicated (Figure 73). This is because the EU health policy only serves to complement national policies, as EU countries hold primary responsibility for organising and delivering health services and medical care. On average, **SMEs see more challenges from additional rules** at the national level, concerning both personal and health data protection. This can be explained by the fact that scaling up operations for cross-border activities demands more effort and more know-how about the local markets, which may be prohibitive for SMEs due to financial constraints and their **lack of expertise and/or capacity to both canvass the national regulatory landscapes and ensure compliance** with all the rules in place.

Figure 73 Additional challenges to the creation of B2B health data marketplaces and unified diabetes-related datasets in the EU stemming from national rules (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

Directly related to data protection and privacy, national rules regarding **professional secrecy and patient-doctor confidentiality** enhance the regulatory framework set up by the GDPR, playing a central role in the trust relationship between patients and doctors.[628] Article 9(3) of the GDPR also stresses that the obligation of secrecy, as defined by national legislation or competent national bodies, must, in any case, be observed for processing health data. As it is the case with the GDPR, patient-doctor confidentiality and professional secrecy support a framework of trust, which is vital for paving the way for data sharing. At the same time, such rules increase the complexity of the regulatory framework that needs to be navigated to set up a data-sharing architecture.[629]

[628] See: Blightman, K., Griffiths, S.E. & Danbury, C. (2014), Patient confidentiality: when can a breach be justified?, Continuing Education in Anaesthesia Critical Care & Pain, Vol. 14(2), pp. 52–56. Available at: https://doi.org/10.1093/bjaceaccp/mkt032

[629] An example in this sense comes from Portugal, where the Data Protection Authority imposed a EUR 400,000 fine on a hospital for non-compliance with the GDPR, notably for the violation of the confidentiality of patients' data and non-conformity with the principle of data minimization. See: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/

Even though the GDPR harmonises the regulatory framework for data protection in the EU, there can still be **differences between how national authorities implement or interpret the GDPR**. Such differences can pose issues for companies operating cross-border and sometimes put more **compliance burden on SMEs**. For example, the GDPR creates a new position, the data protection officer (DPO), with specific requirements and standards to be followed by companies. However, only a few companies actually need to have a formally appointed DPO based on the provisions of the GDPR. The German law implementing the GDPR, however, includes stricter requirements in this sense. Companies with at least 20 employees who deal with the automated processing of personal data need to appoint a DPO.[630]

Finally, there could indeed be a **gap between ethical standards and legal requirements**. While the GDPR provides for a framework to enable derogations when scientific research is concerned, derogations might be seen as challenging in light of ethical standards (explicitly referenced under Recital 33 GDPR) established in other research-related soft legal instruments or international treaties. Research that could be in accordance with the derogations listed in the GDPR might not necessarily be in line with ethical standards that are required by research ethics committees.

Wider policy areas can have an impact on data sharing in the field of health. One important consideration consists of **national rules on data localisation**. Several Member States have rules in place or have been considering rules demanding that certain data should be stored and/or processed on the territory of the country. For instance, Germany requires that metadata related to telecommunications be stored in locations in the country.[631] These requirements raise **operational challenges of data sharing in a cross-border context** and ultimately impede the development of the Digital Single Market. When it comes to health data specifically, while the GDPR notes that special measures can be taken by Member States to ensure the protection of personal data, Recital 53 also stresses that any additional measures and conditions decided by the Member States should not hamper the **free flow of personal data within the EU** when these conditions apply to the cross-border processing of such data.

In addition, a **Regulation on the free flow of non-personal data** was adopted at EU level to lift unjustified limitations and allow for data to be stored and processed anywhere in the EU.[632] While this Regulation does lift some restrictions, the reality is that many datasets nowadays are mixed, containing both personal and non-personal data, raising questions about how this Regulation interacts with the GDPR. In the field of healthcare,

[630] It should be noted that the German law used to be even stricter, requiring that companies with at least 10 employees who deal with the automated processing of personal data need to appoint a DPO. The rule was amended in June 2019. Olsen, Y., Schmidt, D., Schröder, C & Curtis, D. (2019), Germany: New Law Decreases The Number Of Companies Required To Designate A Data Protection Officer In Germany, published on 5 July 2019. Available at: https://www.mondaq.com/germany/data-protection/821920/new-law-decreases-the-number-of-companies-required-to-designate-a-data-protection-officer-in-germany. Last accessed on 6 May 2020.

[631] See: Ben Knight, German data storage laws 'threaten free trade', in Deutsche Welle (DW), published on 12 January 2017. Available at: https://www.dw.com/en/german-data-storage-laws-threaten-free-trade/a-37110699. Last accessed: 6 May 2020.

[632] European Commission (2019), Digital Single Market: Commission publishes guidance on free flow of non-personal data, published on 29 May 2019. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2749. Last accessed: 21 May 2020; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, pp. 59–68. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807

health data can be included in mixed datasets, especially considering the variety of data that is generated, not only in more traditional settings like clinical trials but also through the use of digital health and well-being apps. The guidance provided by the Commission notes that in the case of **mixed datasets**, when the datasets cannot be divided to separate the personal from the non-personal data, the GDPR rules generally apply.[633] This guiding line is especially important for the field of healthcare, as the line between personal and non-personal data is becoming more difficult to distinguish and the utility of a dataset can drastically decrease by separating certain data (see Section 0 for a discussion on data utility and anonymisation).

The creation of **national or EU clouds for data storage** is also very much part of the debate. France has been working since 2012 on the idea of a 'cloud souverain', as an alternative national data storage option for administrations and companies.[634] Germany is currently developing a national cloud, the 'Bundescloud'.[635] A development that has perhaps amplified the discussions in this sense has been the US CLOUD Act,[636] which allows US law enforcement authorities to access data stored by US providers, even if such data is stored outside the US, if the authorities have a mandate in this sense (such as a court order). Questions have been raised about the conflicts between the US CLOUD Act and the GDPR. In particular, if a cloud provider is requested, based on the CLOUD Act, to allow access to personal data stored in the EU, the cloud provider could face the high risk of being sanctioned under the GDPR. Considering the sensitivity of the topic, the highest sanctions envisaged in the GDPR could likely apply.[637] In this respect, the EDPB and the European Data Protection Supervisor issued a joint statement in 2019 on the potential **legal conflict between the GDPR and the US CLOUD Act**. The statement notes that generally, based on Article 48 of the GDPR, a request for accessing data coming from a foreign authority "does not in itself constitute a legal ground for transfer" and that the request can only be recognised in the framework of an international agreement that addresses such cases.[638] To address any conflicts between the two pieces of legislation,

[633] European Commission (2019), Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, (COM/2019/250 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN

[634] The 'cloud souverain' materialised in two cloud providers: Numergy and Cloudwatt. The former was absorbed by the telecommunications company SFR in 2016 for lack of customers, and the latter was officially closed at the end of January 2020 for the same reason. Caulier, S., Numérique : le cloud, enjeu de souveraineté, Le Monde, published on 16 February 2020. Available at: https://www.lemonde.fr/economie/article/2020/02/16/numerique-le-cloud-enjeu-de-souverainete_6029772_3234.html. Last accessed: 6 May 2020; Gros, M., SFR absorbe 100% de Numergy, Le Monde Informatique, published on 25 January 2016. Available at: https://www.lemondeinformatique.fr/actualites/lire-sfr-absorbe-100-de-numergy-63700.html. Last accessed: 6 May 2020.

[635] ITZBund (n.d.), Die Bundescloud: das IT-Fundament der Bundesverwaltung. Available at: https://www.itzbund.de/Webs/DfD/SharedDocs/Projekte/Bundescloud.html. Last accessed: 21 May 2020.

[636] U.S. Clarifying Lawful Overseas Use of Data Act.

[637] Church, P. & Potratz Metcalf, C. (2019), U.S. CLOUD Act and GDPR - Is the cloud still safe?, published on 19 September 2019. Available at: https://www.lexology.com/library/detail.aspx?g=72241f56-b87e-41d5-8a6e-150d09365a25. Last accessed: 6 May 2020.

[638] EDPB and EDPS (2019), ANNEX: Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, p. 3. Available at: https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

the two authorities recommend "an international agreement containing strong procedural and substantive fundamental rights safeguards".[639]

The recent decision of the European Court of Justice (ECJ)[640] to **declare the EU-US Privacy Shield invalid** in July 2020 emphasises even more the sensitivity of data privacy when personal data is transferred from the EU to the US for processing and storage. The EU-US Privacy Shield[641] was a mechanism for such personal data transfers between the EU and the US adopted by the Commission. The ECJ determined that the mechanism does not provide sufficient data privacy and protection safeguards as set by EU law, in particular the GDPR, and thus declared it invalid.[642] On the one hand, this decision could raise **difficulties for SMEs**; approximately 65% of the firms certified through the Privacy Shield are SMEs, allowing them to have data flows between the EU and the US without additional costs for setting special rules and contractual clauses.[643] On the other hand, it makes it clear that the standards for data protection set within the EU need to be respected also in cross-border contexts.

Where and how data is stored is an especially important point for digital health, as a recent case in France shows. The French Health Data Hub, the digital health initiative of the French government which uses AI for drawing novel insights from health data, relies on Microsoft Azure for data storage. This choice has not been free of criticism and it brings up once again the debate on where data should be stored, particularly data as sensitive as health data.[644] It must be noted that Microsoft Azure was awarded the Hébergeurs de Données de Santé (HDS - Health Data Hosting) certification by the French government, a certification that recognises the "strict standards of storing and processing health data for data centres located in France".[645]

---

[639] Ibid., p. 8.

[640] See: Court of Justice of the European Union, Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Case C-311/18. Available at: http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN

[641] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, pp. 1–112. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

[642] See note 640 and Court of Justice of the European Union (2020), "The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield", Press Release No 91/20, 16 July 2020. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[643] Patel, O. & Lea, N. (2020), EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows. Policy Paper, UCL European Institute, p. 12. Available at: https://www.ucl.ac.uk/european-institute/sites/european-institute/files/privacy_shield_brexit_and_the_future_of_transatlantic_data_flows_1.pdf

[644] See: Ceylan, A., Health Data Hub : la légitimité de Microsoft Azure en tant qu'hébergeur de données de santé contestée par un collectif français d'acteurs du secteur du logiciel, Portail de l'IE, published on 20 April 2020. Available at: https://portail-ie.fr/short/2367/health-data-hub-la-legitimite-de-microsoft-azure-en-tant-quhebergeur-de-donnees-de-sante-contestee-par-un-collectif-francais-dacteurs-du-secteur-du-logiciel. Last accessed: 20 May 2020.

[645] See: Microsoft Azure, Microsoft Azure is now certified to host sensitive health data in France, published on 12 November 2018. Available at: https://azure.microsoft.com/nl-nl/blog/microsoft-azure-is-now-certified-to-host-sensitive-health-data-in-france/. Last accessed: 20 May 2020.

Discussions about data localisation are not restricted to individual national initiatives of the Member States. An EU initiative is also shaping up, the **European Cloud Project** (Gaia-X), which is meant to provide a federated, open data infrastructure in the EU.[646]

4.2 Data anonymisation

When it comes to data anonymisation, there is a **trade-off between data privacy and data utility**. Understanding what elements could be used to (re)identify a person (beyond direct identifiers such as social security number or phone number) is challenging and usually underestimated. As **complete anonymisation goes beyond the de-identification of data**, implying the removal of not only obvious attributes from the dataset but also of **quasi-identifiers** (combinations of attributes that could reveal the identities of data subjects), the utility of the data could be compromised in the process.[647]

In the field of health data, one of the reasons explaining the low utilisation of clinical **data published on portals such as the one of the European Medicines Agency** (EMA)[648] is related to the utility of anonymised data. Data must be fully anonymised before being uploaded to the EMA platform for clinical data, which allows, on the one hand, for wide access to the data, but at the same time results in significant data redaction, removing data that could be potentially interesting for stakeholders looking into using the database.[649]

In this discussion, two main approaches to anonymisation exist:[650]

- **Utility-first anonymisation**, which first establishes a suitable level of utility to be conserved after the anonymisation process. The risk of reidentification can then be empirically estimated and the anonymisation process can be repeated changing the model if the estimated risk is deemed too high; and
- **Privacy-first anonymisation**, which selects 'privacy' as a central parameter and limits the reidentification risk. After the anonymisation process, the utility of the data is computed. If the utility is deemed too low, the process can be repeated with a change in the specifications of the anonymisation model.

In those cases when anonymised data have some utility, the **risk of reidentification** may further limit the number and type of information to be included in anonymous datasets. In fact, this risk depends on the sensitivity of the health data in question. In more sensitive

[646] Bundesministerium für Wirtschaft und Energie (2019), Das Projekt GAIA-X: Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems, p. 2. Available at: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=22

[647] Aircloack (2018), Data Anonymisation. What it is and why it matters. Available at: https://aircloak.com/wp-content/uploads/Data-Anonymisation-What-it-is-and-Why-it-Matters.pdf

[648] The Clinical Data portal of the European Medicines Agency brings together clinical data submitted by pharmaceutical companies. See: https://clinicaldata.ema.europa.eu/web/cdp/home

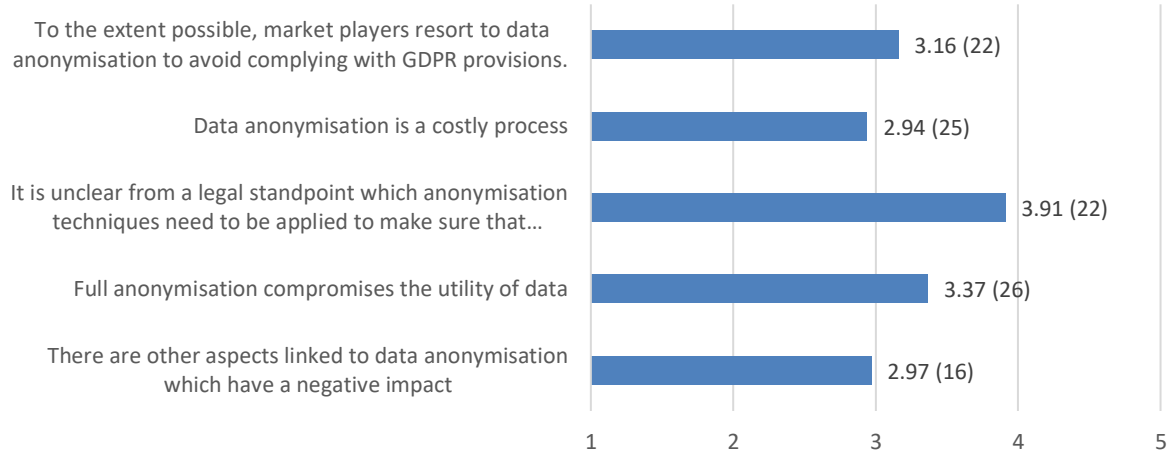
[649] European Medicines Agency (2017), Data anonymisation – a key enabler for clinical data sharing, Workshop Report, p. 3. Available at: https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf

[650] ENISA (2015), Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, p. 29. Available at: https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics

cases (for instance, rare diseases or paediatric patients), special provisions to limit this risk could be needed to effectively balance privacy and utility, as well as obtain the consent of data subjects for data sharing.[651]

As anonymisation renders data non-personal, anonymisation techniques could be employed to avoid having to comply with the requirements of the GDPR.[652] The stakeholders consulted for this Study noted that while this possibility exists and actors may resort to it in certain cases (see Figure 74), the decision to anonymise data very much depends on the situation at hand. The costs involved with setting up a system to anonymise data are not the problem in themselves, and they raise only a few challenges (see Figure 74), such as the initial costs for getting the system running or for calibrating as needed. The actual problem is the **selection of the most appropriate anonymisation techniques**, especially to comply with the GDPR. The **reliability of data anonymisation** may also be an additional potential obstacle to gaining the trust of users who are seeking assurances regarding the governance of the data, given, in particular, the sensitivity of personal health information.[653]

Figure 74 Challenges related to data anonymisation (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

The consulted stakeholders pointed out that it is not clear, from a legal standpoint, which anonymisation techniques need to be applied to make sure that relevant data is not considered anymore personal data, thus falling outside the scope of application of the GDPR. Some organisations, especially those with a longer standing in the market, have processes in place that make such questions relatively easier to address. This may not be as straightforward for a **start-up or SME**, especially those who seek to exploit an innovative service to make it in the market. In the **absence of clear legal guidelines**,

[651] See note 650, p. 25.

[652] Recital 26 of the GDPR mandates that "the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".

[653] European Commission (2014), The use of Big Data in public policy research – Background information document, p. 10. Available at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20141118_co07b_en.pdf

one factor that can be taken into consideration in the process of anonymising data is commercial risk. Depending on how the risk is assessed by different stakeholders, a stance more prudent than necessary may in the end **inhibit innovation or give rise to asymmetric positions of stakeholders**. Against this background, as a given entity may be held liable in case of reidentification of data released to another entity, **the commercial risk appears to be quite high**, thus calling for a reliable anonymisation process, compliant with the GDPR.[654]

More guidance would be thus needed on this topic, taking into consideration also the variety of applications that data in the field of healthcare can have for the development of innovative services. In 2014, the Article 29 Working Party on data protection issued an opinion on 'Anonymisation Techniques',[655] adopting the privacy-first approach and listing a set of criteria for anonymisation. With the entry into force of the GDPR, the principle of 'data protection by design and by default' was introduced.[656] However, unlike the **US Health Insurance Portability and Accountability Act** (HIPAA), which describes two potential methodologies to achieve de-identification of data, the GDPR does not suggest any specific approach. In this regard, the European Data Protection Board (EDPB) and the national data protection authorities (DPAs) could play an important part in the implementation of the GDPR, by offering their guidance and helping **avoid heterogeneous approaches to anonymisation stemming from different interpretations of the GDPR**.

Additional questions arise when looking strictly at anonymisation in the context of the **secondary use of health data** and GDPR implications. There are two possible approaches concerning what constitutes anonymised data for secondary use, such as research.[657] The first approach considers that it is possible to anonymise health data for secondary uses while **allowing a different data controller the possibility to reidentify the data subject if necessary.** In other words, it should be possible to anonymise data as far as research activities are concerned (for instance by replacing identifiable data with a code), but leaving the option for a separate entity holding the encryption key to reidentify the patient if needed (by re-matching the code with the identifiable information). This would allow for necessary, medically actionable information to be passed to a clinician who may then contact the data subject. The **second approach is stricter with regard to anonymisation**: as long as someone has the key to decrypt the data and reidentify the person, then the data is considered personal for everyone. The GDPR rather adheres to the second, stricter approach. In this respect, Recital 26 of the GDPR states that "personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person",[658] to which the data protection

[654] See note 649.

[655] Article 29 Data Protection Working Party (2014), Opinion 05/2014 on Anonymisation Techniques. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. The Working Party ceased to exist in May 2018, when the GDPR entered into force, and was replaced by the European Data Protection Board.

[656] See GDPR, Article 25 (see note 608).

[657] This issue was brought up during the interviews conducted for this study. The problem is also documented in the following article: Peloquin, D., DiMaio, M., Bierer, B. & Barnes, M. (2019), Disruptive and avoidable: GDPR challenges to secondary research uses of data, European Journal of Human Genetics, 28. Available at: https://doi.org/10.1038/s41431-020-0596-x

[658] GDPR, Recital 26 (see note 608).

principles apply. **Pseudonymisation** refers to the process of replacing personally identifiable attributes in a record with artificial attributes or pseudonyms in such a way that the data can no longer be attributed to a data subject without additional information.[659]

Against this background, the questions around anonymisation and pseudonymisation stem from the fact that the GDPR is a piece of legislation with general applicability and may not be able to always capture the specificities of certain sectors, such as health data sharing and implications for research. Given the complex interaction between the GDPR and the need to further enable the secondary use of health data, more guidance from the EDPB could be beneficial to ensure that unnecessary hurdles to research are removed.[660]

An additional level of complexity, but very relevant for the debate, consists of how data may be **reused for future research and projects**. Trimming a dataset to fulfil anonymisation requirements does not take into consideration the potential of the data for future projects. As such, the data, once anonymised for specific purposes, may not be usable in the future or the anonymised dataset may not allow for additional data to be added and matched with the original data subjects, since identifiers were removed.

The discussion on how anonymisation should be carried out is also linked to the **right to be forgotten** (Article 17 of the GDPR). For instance, should all personal data be erased or can anonymisation also be considered as fulfilling a request advanced by a data subject based on this right enshrined in the GDPR? A recent decision by the Austrian Data Protection Authority (DPA) addressed this issue.[661] The Austrian DPA noted that **anonymising personal data can in principle be used as a method to erase personal data** and thus comply with Article 17, provided that a request from a data subject is put forward in this sense. The decision also specifies that the anonymisation process must be carried out in such a manner that neither the data controller nor any other third party could reidentify the data subject from the anonymised and remaining data.

Nevertheless, with ever-evolving technologies and data processing techniques, some researchers draw the attention to the fact that a level of anonymisation that, on the one hand, maintains utility for the research or commercial purposes and, on the other hand, guarantees that data subjects can in no way be reidentified is very difficult to achieve. A 2019 paper provides an example of how data can be reidentified and estimates the **likelihood of reidentification** by employing and training a statistical model based on a 'heavily' incomplete dataset.[662]

[659] GDPR, Article 4(5) (see note 608).

[660] Peloquin, D., DiMaio, M., Bierer, B. & Barnes, M. (2019), Disruptive and avoidable: GDPR challenges to secondary research uses of data, European Journal of Human Genetics, 28, pp. 697–705. Available at: https://doi.org/10.1038/s41431-020-0596-x

[661] Data Protection Authority, Austria, Decision of 5 December 2018, DSB-D123.270/0009-DSB/2018. Available at: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html

[662] Rocher, L., Hendrickx, J.M. & de Montjoye, Y. (2019), Estimating the success of reidentifications in incomplete datasets using generative models, Nature Communications, Vol. 10, 3069. Available at: https://doi.org/10.1038/s41467-019-10933-3

4.3 Liability rules

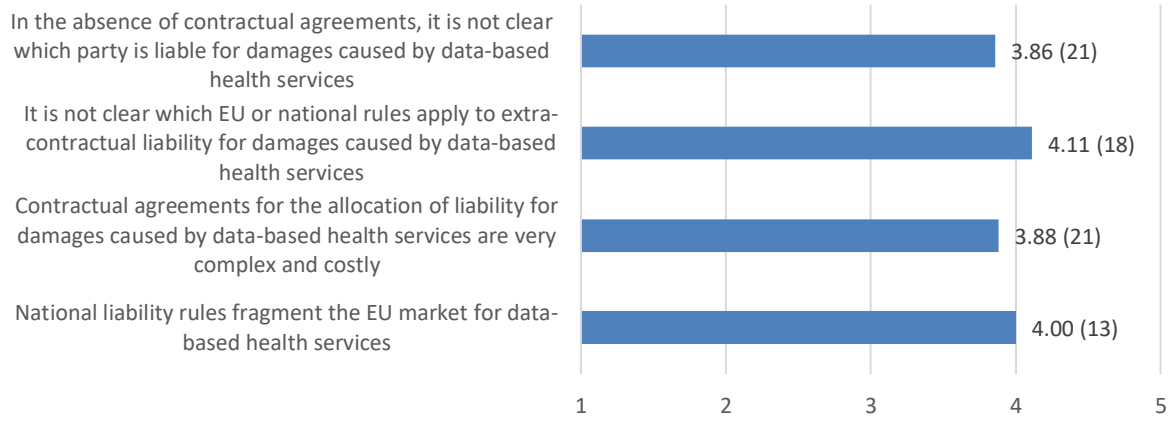
Legal liability comes in two forms: i) extra-contractual liability, referring to the rules set in the general legal framework, outside of contracts, including EU rules in the field; and ii) contractual liability, i.e. the liability assumed by parties entering a contractual agreement.

Extra-contractual liability

At the EU-level, several pieces of legislation are relevant, some applying more generally to liability issues, such as the Product Liability Directive,[663] and others being specific to the field of health, as it is the case with the Medical Device Regulation.[664] For breaches of data privacy, the rules set out in in the GDPR apply, as discussed in Section 0.

The Product Liability Directive and the Medical Device Regulation help create an EU framework of liability in the field, but **uncertainties surrounding extra-contractual rules** still remain, as consulted stakeholder have also emphasised. The stakeholders noted that there may be some cases in which, in the absence of contractual agreements, it is not clear which party is liable (e.g. service provider, data provider) for **damages caused by data-based health services** (see Figure 75), given the novelty of the field. In addition, the stakeholders pointed out that it is not clear which EU or national rules apply to extra-contractual liability (see Figure 75). According to the interviews, **for SMEs these challenges are more burdensome** compared to other stakeholders in the field.

Figure 75 Challenges related to liability (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

The **Product Liability Directive** of 1985 defines a **regime of strict liability in the EU**, under which a producer may be liable for damages caused by defective products, without

[663] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products OJ L 210, 7.8.1985, pp. 29–33. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374

[664] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017, pp. 1–175.

the need to establish negligence or fault on the producer's part.[665] The recent developments in the field of digital economy have brought uncertainty with regards to **liability rules applied specifically to data sharing**, as EU rules in the field were originally designed to apply to tangible goods. Can applications be considered products? What digital services should be covered by EU legislation on liability? The challenges that have arisen can be seen from two perspectives:[666]

- From the **perspective of the data providers**, liability risks are perceived in particular when it comes to the sharing of data and the potential misuse of data by third parties;
- From the **perspective of reusing or accessing the data**, liability risks are identified with respect to the reliability of data and to potential issues that may arise from reusing incorrect data.

Against this background and considering the challenges brought by the emergence and subsequent expansive growth of the digital economy from 1985 to the present, the relevance and fitness for purpose of the Product Liability Directive were recently assessed by the Commission as part of the policy evaluation process. The evaluation confirmed that **the application of the Directive may be challenging or uncertain when it comes to emerging digital technologies**, and as such the Directive should be adapted.[667]

Looking more in depth into the additional challenges brought by emerging digital technologies, the question of **cybersecurity and the impact that cyberattacks** have on liability is also relevant. The risk of cyberattacks increases the complexity of how to assign liability and whether the service provider should be held directly liable for damages coming from the cyberattack or whether the wider picture should be considered. As noted in a Commission Staff Working Document, a framework for liability in this sense should consider to what extent the operator abides by cybersecurity standards.[668]

When it comes to eHealth applications, the **Medical Device Regulation**[669] (which came into force on 25 May 2017 and will become fully applicable on 26 May 2021)[670] sets out

[665] See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al32012

[666] Deloitte et al. (2016) for the European Commission, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, pp. 81-82. Available at: https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and

[667] European Commission (2018), Commission Staff Working Document, Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, (SWD/2018/157 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018SC0157

[668] European Commission (2018), Commission Staff Working Document, Liability for emerging digital technologies, (SWD(2018) 137 final), p. 20. Available at: https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies

[669] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017, pp. 1–175. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745

[670] The Regulation was initially scheduled to become fully applicable on 26 May 2020, but its application was delayed by the Commission in April 2020 due to the COVID-19 pandemic. See: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_589

rules for ensuring the quality and safety of medical devices, monitoring the performance of devices once on the market, as well as enhancing the transparency of information vis-à-vis consumers. Compared to the previous EU rules in the field set out in the Medical Device Directive, the Regulation, *inter alia,* expands the definition of medical devices to include devices, both hardware and software, designed for the purposes of prediction and prognosis of a disease, introduces new criteria for the risk classification of devices to enhance safety as well as an enhanced system for vigilance and post-market surveillance for transparency and safety.[671]

Going more into detail, the question still remains of what types of products and services fall under the scope of the Medical Device Regulation. With new technologies and new applications in the field of healthcare, can, for instance, a lifestyle app be subject to the provisions of the Regulation? The Regulation covers a **wide range of applications**, namely "any instrument, apparatus, appliance, software, implant, reagent, material or other article" with the distinctive feature that the manufacturer expressly intended the application to be used for a **specific medical purpose**, as defined by the Regulation (for instance, "diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease").[672] The way the purpose of the app is defined by the manufacturer is, as such, the important point to consider as software created for medical purposes will be subject to the Medical Device Regulation. Conversely, software meant by the manufacturer for "general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device".[673] As **well-being apps are not covered by sector-specific legislation**, consumer law may step in for regulating any issues that may arise.[674]

Finally, an emerging but challenging field, from a legal point of view, is the use of **AI in healthcare**. Applications based on AI technology may bring another layer of complexity, raising questions about how to test and approve such applications, who would be held liable for potential damages resulting from their use, what role the practitioners play, and how to ensure the transparency of processes.[675]

Contractual liability

Uncertainties stemming from extra-contractual liability could be addressed in a different way. Contractual liability could be the preferred option for businesses to ensure a **certain level of risk minimisation when working with data**. While contracts may provide a

[671] See: European Hospital and Healthcare Federation (2017), Analysis of the new Medical Devices Regulation (MDR) and In vitro diagnostic Medical Devices Regulation (IVDR) draft texts. Available at: http://www.hope.be/wp-content/uploads/2017/01/104_2017_HOPE-ANALYSIS_Analysis-MDR-and-IVDR-draft-texts.pdf

[672] Medical Device Regulation, Article 2 (see note 664).

[673] Medical Device Regulation, Recital 20, ibid. The Commission has also published additional guidance on the application of the Regulation. See: http://ec.europa.eu/DocsRoom/documents/17921/attachments/1/translations

[674] Bächle, T.C. & Wernick, A. (eds.) (2019), The futures of eHealth. Social, ethical and legal challenges, Alexander von Humboldt Institute for Internet and Society (HIIG), p. 11. Available at: https://www.hiig.de/publication/the-futures-of-ehealth-social-ethical-and-legal-challenges/

[675] Kiseleva, A. (2019), Decisions made by AI versus transparency: Who wins in healthcare?, in Bächle, T.C. & Wernick, A. (eds.) (2019), The futures of eHealth. Social, ethical and legal challenges, Alexander von Humboldt Institute for Internet and Society (HIIG), pp. 93-97. Available at: https://www.hiig.de/publication/the-futures-of-ehealth-social-ethical-and-legal-challenges/

solution, it tends to be quite **complex and also costly** to ensure that the resulting document is comprehensive, as reflected by the feedback from the consulted stakeholders (see Figure 75). In addition, this may be an **impediment for SMEs** who may not have the capacity to act in this sense and may have **limited bargaining power** to negotiate favourable contractual terms.

In this regard, the European Commission issued **guidelines for sharing private sector data**, which also identify liability provisions that could be taken into consideration when preparing data usage agreements. In particular, the Commission suggests including provisions referring to the "supply of erroneous data, disruptions in the data transmission, low-quality interpretative work, if shared with datasets, or for destruction/loss or alteration of data (if it is unlawful or accidental) that may potentially cause damages".[676]

National liability rules

Beyond EU-level rules for liability, national liability rules can add another layer of complexity, as the consulted stakeholders emphasised (see Figure 75). Fragmentation is likely to occur especially considering that **health law is not harmonised in the EU**, and neither is contract law, beyond the existence of guidelines issued by the Commission for specific issues, such as sharing private-sector data. Different national rules implemented by Member States can lead to a **fragmented legal landscape**, thus creating hurdles for companies, especially in a cross-border context.[677] In some cases, **further legal fragmentation can occur within a country**. In Germany's federal system, healthcare policy is also, at least partly, a question for the Länder,[678] which can lead to different standards being applicable at state level. Recently, discussions in Germany on lifting some restrictions concerning telemedicine emphasised the fragmentation that can occur within a country.[679]

Nevertheless, **national measures may also be drivers of change**. In 2019, Germany adopted the Digital Healthcare Act (Digitale-Versorgung-Gesetz), taking important steps towards supporting the deployment of eHealth applications. Notably, the Act gives the possibility for doctors to prescribe digital therapeutics, such as health apps, to patients and for them to be reimbursed by the statutory health insurance. The apps first undergo a **check in terms of security, functionality, quality, and data security and privacy** by the Federal Institute for Drugs and Medical Devices, after which they are made available for prescription and reimbursement for one year. Within the first year of their availability for prescription, the app manufacturer must **provide evidence that the app improves healthcare provision**. In addition, health insurance funds can also invest in innovative eHealth applications through targeted funding or participation in venture capital funds.[680]

[676] European Commission (2018), Commission Staff Working Document, Guidance on sharing private sector data in the European data economy, (SWD(2018) 125 final). Available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy

[677] See note 674, p. 11.

[678] Similarly, in Italy the regional governments are responsible for the implementation of healthcare policy, with the national government overseeing that the general objectives are met. See: https://www.euro.who.int/en/countries/italy

[679] See note 674, pp. 173-175.

[680] Bundesministerium für Gesundheit (n.d.), Ärzte sollen Apps verschreiben können, Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG), last updated on 22

An initiative like the German Digital Healthcare Act may support wider adoption of similar measures and thus help bolster market opportunities in Germany and also more widely in the EU. While the Act does require that manufacturers provide proof of the effectiveness of the apps deployed, it leaves **questions concerning liability open**. For instance, the prescribing doctor is generally liable in the relationship with the patient under the treatment contract, but in the case of new apps for which risks may be unknown to the doctor, the liability burden is unclear. For the app manufacturer, as discussed above in the context of extra-contractual liability, **legislation in the area of medical devices** applies. In addition, there is a need for adapting **product liability legislation** to the challenges of digitalisation.[681]

National rules and standards may add complexity to the legal system, but they can be just as important in **creating the space for trust** that is needed when working with sensitive healthcare data. For instance, the French National Agency for Digital Health introduced the **HDS certification for providers hosting health data for third parties** in France. The certification ensures that standards for the security and confidentiality of health data are in place.[682]

A framework for ensuring data quality in the marketplace context

Liability rules are thus complex, especially when one considers the full picture of **determining liability in the healthcare sector** where emerging technological developments bring up the need for further guidance and clarity. The interplay between different stakeholders in the system, including insurances, adds another layer of intricacy.[683]

An EU-wide B2B marketplace for data sharing in healthcare would need to consider the role of different stakeholders when it comes to liability issues stemming from poor data quality. A framework for determining **responsibility for the quality of data** shared in the marketplace is therefore needed. To assign responsibility vis-à-vis the quality of data in the context of a B2B health data marketplace, three main categories of stakeholders can be considered: the data providers, the owners of the B2B health data marketplace, and the providers of data-based healthcare services. The feedback from the consulted stakeholders, as reflected in Figure 76, shows that, in principle, **the main responsibility for the quality of data should lie with the data providers**. The argument for this is straightforward: as data providers bring the data into the marketplace making them accessible (subject to the potential rules of the marketplace) to other parties, they need

April 2020. Available at: https://www.bundesgesundheitsministerium.de/digitale-versorgung-gesetz.html. Last accessed: 21 May 2020.

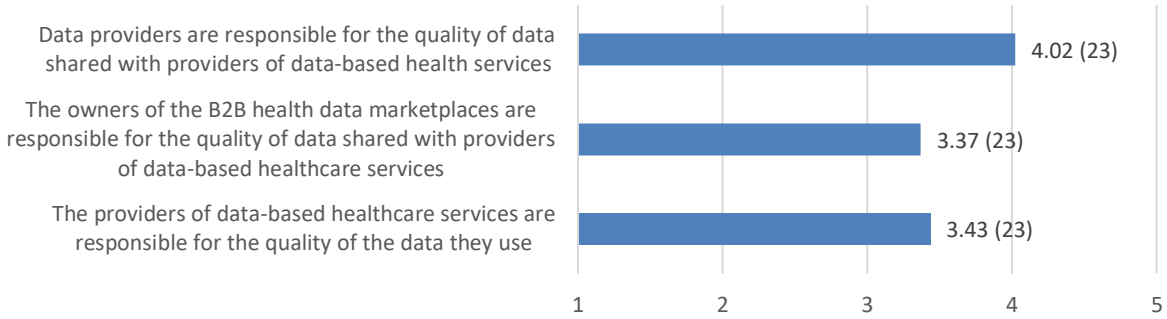
[681] Reinhard, T. & Mößmer, L. (2020), Germany introduces new Digital Healthcare Act: Health apps now available on prescription, published on 14 May 2020. Available at: https://www.lexology.com/library/detail.aspx?g=272e7f0a-0294-4170-bb5a-b049fd403f54. Last accessed: 26 June 2020.

[682] Agence du numérique en santé (n.d.), Labels et certifications : Hébergement des données de santé. Available at: https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante. Last accessed: 21 May 2020.

[683] Expert Group on Liability and New Technologies – New Technologies Formation (2019) for the European Commission, Liability for Artificial Intelligence and other emerging digital technologies, p. 18. Available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

to ensure that, to the best of their knowledge, the data are of good quality, without underlying mistakes that may lead to issues when data are reused.

Figure 76 Extent to which different stakeholders can be considered responsible for the quality of data shared (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

Through the interactions between data providers, marketplace owners, and providers of data-based services, however, a **chain of responsibility** ensues. For instance, the **marketplace owners** could hold some responsibility for ensuring the governance of the system and the rules and principles for e.g. data providers to input data in the marketplace and validate them. In a field where trust is crucial, a **well-defined governance framework** will play an important part in making the system work. During the interviews, most of the **consulted SMEs** (some of them acting as data intermediaries) put much less emphasis on the responsibility of the marketplace owners and rather emphasised more their role as facilitators and enablers of data sharing. Finally, while the **providers of the data-based services** should be liable for any issues that arise from the processing of data, they could also be held responsible for assessing the quality of the data on which their service relies, especially if one considers that they are bound by a **relationship of direct proximity** (and trust, as further discussed in the next Section) with the final users of the service.[684]

While some answers in this exercise of assigning responsibility may be straightforward, an EU-wide B2B health data marketplace would benefit from **clear guidelines to reduce litigation costs**, **instil trust** in the system and **convince stakeholders to participate**.

[684] A relationship of proximity is a central element to determine legal liability in a fault-based system according to both the so-called Caparo test (https://www.bailii.org/uk/cases/UKHL/1990/2.html) and Anns test (https://www.bailii.org/uk/cases/UKHL/1977/4.html).

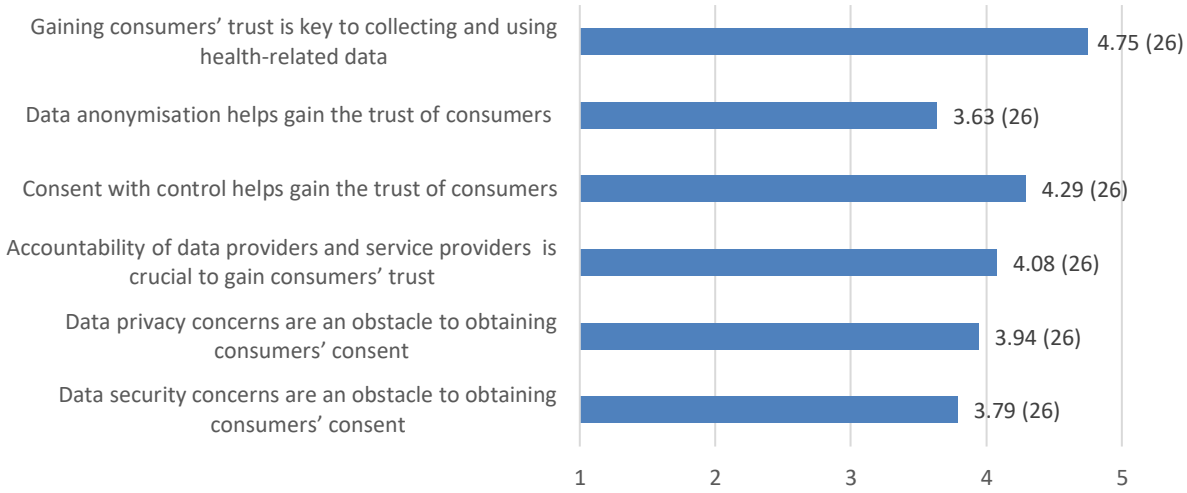
5. Accountability and trust

Trust is the common thread surrounding the main challenges to data sharing in the health sector. For new services to be developed and to be taken up in the market, **gaining the trust** of patients and, more generally, of consumers, is essential. The stakeholders consulted for this Study agreed across the board that this is a *sine qua non* for the provision of data-based services in the field of health (see Figure 77). The importance of trust in this field stems from the fact that the processing of personal and health-related data is not only a question of legality, but also a **question of ethics**, especially in research and clinical trials.

There are several ways in which a service provider can gain the trust of consumers, at least theoretically. These include:

- Designing a **framework for consent with control** (giving individuals the option to retrieve and retract the information provided);
- Implementing **rules for the accountability** of service providers and data controllers (i.e. their ability to share evidence with consumers about the measures they apply to comply with data protection rules and principles);
- **Addressing data privacy and security concerns**; and
- Putting in place **processes for data anonymisation** (to assure individuals of the privacy of their data).

Figure 77 Methods and obstacles to gaining consumers' trust (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

Consent with control

Consent with control, or dynamic consent, is a newer concept facilitated by digital technologies, mainly applied for the secondary use of data for research and clinical trials. **Dynamic consent** can be a promising option for building trust, with advantages such as increasing the engagement of individuals for activities involving the secondary use of data, facilitating interactions between researchers (data controllers) and participants in research activities (data subjects), embedding high legal and ethical standards, transparency, and

more options for individuals to decide whether to share or withdraw their data.[685] The consulted stakeholders see the potential of this option to mitigate trust issues that individuals might have when sharing their data (see Figure 77).

Dynamic consent facilitates the way individuals engage and share their data, in particular health-related data, for research, shifting the focus to a more **user-centric experience**. Dynamic consent "enables participants to consent to new projects or to alter their consent choices in real-time as their circumstances change and to have confidence that these changed choices will take effect."[686] This allows for continued interactions between, for instance, individuals participating in research activities and the data controllers in the research team. This model could be exported to other settings, such as data-based services, allowing individuals to be more involved in what type of data they share and with whom.

While there are **advantages for engagement and building trust**, dynamic consent may raise **challenges to the research process**. For instance, if participants withdraw their data as research is ongoing, the project results may be affected.

Accountability

Ensuring a high level of accountability of the data controllers and processors (namely those entities tasked with processing data on behalf of the data controller) appears to be a prerequisite for gaining the trust of individuals. Building on the discussion about data protection, accountability aims to **guarantee and provide evidence** to show that the practices of data controllers do indeed comply with data protection principles. Accountability requires that **internal control systems** be put in place to produce evidence in this sense (for instance audit reports), which can be presented to data subjects, supervisory bodies, and other stakeholders.[687] Accountability issues can be particularly problematic when it comes to mHealth solutions (for instance smartphone apps) if they fail and harm the interests of patients.[688]

The consulted stakeholders consider accountability to be highly relevant as well, as reflected by the average answers presented in Figure 77. This includes having **transparency**, **clear data governance**, **and clear procedures** in place for individuals to be able to flag when they believe something is wrong in how their data is processed and used. Importantly, however, accountability and transparency should not result in an overflow of information that is difficult to digest. The information provided should be clear, concise, and the language used should be **accessible to a general audience**.

In addition, in a research setting, transparency could also be enhanced by ensuring there is a **feedback loop**, providing information to the participants about the research results.

[685] Kaye, J., Whitley, E., Lund, D. et al. (2015), Dynamic consent: a patient interface for twenty-first century research networks, European Journal of Human Genetics, Vol. 23, pp. 141–146. Available at: https://doi.org/10.1038/ejhg.2014.71

[686] Ibid.

[687] See note 649, p. 10.

[688] CDTM (2016), Digital Innovation in Diabetes Care. Trend Report, p. 25. Available at: https://www.eithealth.eu/documents/21805/0/Trend+Report+on+Diabetes/a2bf8334-c401-4671-8ddd-9589bf00bf99

This can generate more involvement and engagement of individuals throughout the research process, thus building more trust.[689]

When it comes to relevant rules in the area, the GDPR introduced **requirements for data processors**. In particular, Article 28.1 of the GDPR states that controllers "shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject". In the same vein, Article 89 of the GDPR, focusing specifically on the situations in which personal data is used for research purposes, notes that data processing in this case is subject to "appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject".

Data privacy and security concerns

Data privacy and security concerns could be an obstacle to obtaining user consent for gathering and processing health data or sharing them with third parties – whether it is patient data or data obtained through digital devices and wearables. Surveys focused on mHealth and wearable devices revealed that **concerns about privacy and the threat of security breaches** are highly important for potential users.[690] The attitude of users vis-à-vis data-driven healthcare and wearables implies higher standards of privacy and security need to be ensured, especially when it comes to:

- **Data access**: ensuring accessibility through secure transmission channels; and
- **Data storage**: providing a secure location for storing the data.

Stakeholders interviewed for this Study confirmed that data privacy and security concerns can pose some challenges to obtaining individuals' consent for using and processing their data (see Figure 77). With recent scandals involving the sharing of personal data, such as the Cambridge Analytica scandal,[691] these issues are likely to become more salient to the general public. Therefore, it is important for stakeholders to **acknowledge such concerns and mitigate them** through, for instance, more accountability and transparency about the processes in place to prevent data breaches as well as the access of unauthorised third parties to the data.

A recent case in the UK involving the NHS and DeepMind (a company owned by Google) illustrates the need for transparency. In a partnership with Google's DeepMind for developing an app for monitoring patients with kidney disease, the NHS shared with DeepMind data on 1.6 million NHS patients without properly informing the patients about

[689] Spencer, K., Sanders, C., Whitley, E.A., Lund, D., Kaye, J. & Dixon, W.G. (2016), Patient Perspectives on Sharing Anonymized Personal Health Data Using a Digital System for Dynamic Consent and Research Feedback: A Qualitative Study, Journal of Medical Internet Research, Vol. 18(4). Available at: https://doi.org/10.2196/jmir.5011

[690] European Commission (2014), Green Paper on mobile Health. Available at: https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth; PWC (2014), The Wearable Future, Consumer Intelligence Series. Available at: https://www.pwc.se/sv/pdf-reports/consumer-intelligence-series-the-wearable-future.pdf

[691] See: Confessore, N., Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times, published on 4 April 2018. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Last accessed: 20 May 2020.

how their data would be used.[692] Reportedly, the anonymised data that was shared contained information about medical history, religion, and ethnic origin.[693] In this context, a report published by the University of Manchester in 2020 highlights the "complexity and fragility" of health data sharing, calling for more action from "the NHS, the government, universities and companies to avoid damaging public trust in health research".[694]

A 2019 study investigated how user data are shared by health apps for Android, which are available to download in the United Kingdom, United States, Canada, and Australia. The study found that **data sharing practices are lacking in transparency and entail privacy risks**, noting that clinicians recommending certain health apps should also make individuals aware of the potential risks to privacy that apps carry. At the same time, the study also noted that the implementation of the GDPR in the EU "resulted in greater transparency around data sharing relationships" (for an in-depth discussion on the GDPR, see Section 0).[695]

At the EU level, preparations for a **Privacy Code of Conduct on mHealth apps** were initiated by the Commission in 2015 to address trust issues related to mHealth apps. Submitted for approval to the Article 29 Working Party, the Code was found to be unfit in view of the entry into force of the GDPR in 2018 (which set higher standards than the Code) and thus was not approved. Nevertheless, the Commission encourages stakeholders to continue the cooperation in this field to further develop the Code of Conduct.

To increase transparency and address potential concerns around data privacy and security, one solution that could be adopted is a '**privacy label' for health apps**.[696] Such a label could contain information about the underlying technology and the level of privacy of the application in a clear and distilled fashion, similar to nutrition labels. This would also **raise the level of awareness** among individuals about data processing and data privacy. In addition, an app label can be a **self-regulatory measure**, allowing developers to distinguish themselves through the importance they give to the security and privacy of the user data that is shared through the app.[697]

---

[692] Information Commissioner's Office (ICO) (2017), Royal Free - Google DeepMind trial failed to comply with data protection law, published on: 3 July 2017. Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/. Last accessed: 21 May 2020.

[693] Vaughan, A. (2019), Google is taking over DeepMind's NHS contracts – should we be worried?, New Scientist, 27 September 2019. Available at: https://www.newscientist.com/article/2217939-google-is-taking-over-deepminds-nhs-contracts-should-we-be-worried/. Last accessed: 21 May 2020.

[694] University of Manchester (2020), We need to re-think health data sharing and public trust, published on 28 January 2020. Available at: https://www.manchester.ac.uk/discover/news/we-need-to-re-think-health-data-sharing-and-public-trust-says-pub/. Last accessed: 21 May 2020.

[695] Grundy, Q., Chiu, K., Held, F., Continella, A., Bero, L., Holz, R. et al. (2019), Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis, BMJ 2019, Vol. 364 :l920. Available at: https://doi.org/10.1136/bmj.l920

[696] The Finnish Innovation Fund Sitra has also put forward the idea of introducing a more general app label for the digital economy, the "fair data label", informing users about how the service complies with data protection and reuse rules. See: Ilves, L.K. & Osimo, D. (2019), A Roadmap for a Fair Data Economy. Policy Brief, Sitra, p. 47. Available at: https://media.sitra.fi/2019/04/09132843/a-roadmap-for-a-fair-data-economy.pdf

[697] Bates, D. W., Landman, A. & Levine, D. M. (2018), Health apps and health policy: what is needed?, JAMA, Vol. 320, pp. 1975–1976. Available at: https://doi.org/10.1001%2Fjama.2018.14378

With regard to **cybersecurity**, the field of health falls under the incidence of the Directive concerning measures for a high common level of security of network and information systems across the Union (**NIS Directive**).[698] The Directive sets out **security and notification requirements** for operators of essential services as well as for digital service providers, such as cloud computing services. In the field of healthcare, **hospitals are considered to be operators of essential services** and as such they need to prevent and minimise the impact of disruptions affecting the security of their systems and take technical and organisational measures to reduce the risk posed to the security of their network and information systems. **Digital service providers** face relatively softer requirements compared to the operators of essential services;[699] they are required to adopt security measures in line with **international standards** and notify incidents that have a substantial impact on the provision of services.

There can be an **interplay between the NIS Directive and the GDPR** when personal data are involved. While the NIS Directive was adopted at the same time as the GDPR, the two pieces of legislation do not reference each other in their respective texts. Nevertheless, whenever personal data are handled by either operators of essential services or digital service providers, both pieces of legislation need to be considered. The **compliance requirements are assessed separately**,[700] which may increase the **regulatory burden** for stakeholders, and **particularly for SMEs**.

Data anonymisation for trust

Finally, **data anonymisation is deemed less important than accountability or consent with control** for gaining the trust of consumers, based on feedback from the consulted stakeholders. As outlined in Section 0, anonymisation is a complex task that still leaves some questions open, such as the **risk of reidentification**. Given the complexity of the process and the adverse impact on the utility of data, anonymisation may not be the best method to put the concerns of patients and individuals at rest about how their data is processed. Data governance and transparency are more important. As highlighted throughout this Section, several studies have shown that being transparent about the processes in place for sharing and protecting data, as well as enabling a feedback loop between the individual and the data controllers and data processors are seen as good practices for instilling trust and encouraging more individuals to share their data.

[698] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

[699] Markopoulou, D., Papakonstantinou, V. & De Hert, P. (2019), The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review 35(6). Available at: https://doi.org/10.1016/j.clsr.2019.06.007

[700] Ibid.

6. Interoperability

Health data sharing requires not only a clear framework of rules and principles for data protection, liability, and accountability, but also the models, processes, and infrastructure to enable data to flow between systems and to be correctly interpreted. This Section explores the *status quo* of the interoperability of health data and the need for a consistent take-up of standards to enable data sharing.

6.1 Limited interoperability and associated costs

With the rise of digitisation and new technologies, more and more data are generated in the healthcare sector. However, in the absence of a common framework for defining, structuring, and sharing data, their full potential is not realised. The **lack of a common framework and uptake of standards in the field of digital health** are potential barriers to the deployment of data-driven solutions and the move towards person-centred healthcare.

Interoperability is "the ability of two or more systems or components to exchange information and to use the information that has been exchanged".[701] Interoperability comes in different shapes and forms and is generally seen as consisting of four layers: legal, organisational, semantic and technical. **Legal interoperability** designates the need for a coherent legal and regulatory framework allowing the exchange of data between different systems, countries, etc.[702] Any barriers that can arise in this field (for instance, fragmentation at the level of national legislation) are discussed in Section 4. **Organisational interoperability** refers to the procedures and policies in place in organisations that allow them to cooperate and exchange information,[703] defining how the different actors in the health data ecosystem interact. **Semantic interoperability** designates the ability of information exchanged between systems to be interpreted without ambiguity.[704] Specifically in the field of health, this refers to data models and standards, as well as medical terminologies and ontologies.[705] Finally, **technical interoperability** requires that the technical means are in place to allow data transfers between systems, such as digital networks and relevant communications protocols.[706]

Against this background, **interoperability-related barriers** may stem from, *inter alia*, the lack of standards to facilitate the storage, transfer and processing of data as well as from lack of or outdated technical infrastructure. Such barriers particularly appear when companies start to be involved in B2B data sharing. Interoperability has been identified as one of the primary barriers in data sharing and reuse in the EU. A survey carried out by

---

[701] IEEE Standard Computer Dictionary, A Compilation of IEEE Standard Computer Glossaries, IEEE Std 610 1-217 (1991). Available at: https://doi.org/10.1109/IEEESTD.1991.106963

[702] eHealth Governance Initiative (2012), Discussion Paper on Semantic and Technical Interoperability, p. 1. Available at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20121107_wd02_en.pdf

[703] Bincoletto, G. (2020), Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union, Data & Policy, Vol. 2, E3, p. 3. Available at: https://doi.org/10.1017/dap.2020.2

[704] See note 702.

[705] Lehne, M., Sass, J., Essenwanger, A. et al. (2019), Why digital medicine depends on interoperability, npj Digital Medicine, Vol. 2, 79, p. 2. Available at: https://doi.org/10.1038/s41746-019-0158-1

[706] Ibid.

Deloitte, for example, has found that 51% of the respondents (data users and (re-)users) identified the lack of interoperability and technical standards as a "blocking factor, or very important or considerable barrier" preventing them from deploying new business models.

Stakeholders consulted for this Study unanimously agree that the lack of interoperability is a highly significant challenge for creating B2B platforms and unified diabetes-related datasets at the EU level (see Figure 78). This is due to the fact that data sharing and unified datasets by definition require that systems be able to communicate with one another. The current landscape of health data is, however, very fragmented and characterised by **incompatible IT systems**, **different data formats**, and **data silos** which make it difficult to tap the full potential of data.[707] The size of the problem becomes evident when one takes into account the **multiple data sources** that exist (clinical data, traditional patient-generated data, digital biomarkers coming from a variety of devices, etc.) and the **multiple stakeholders** who interact in the field (hospitals, associations of patients, data intermediaries, and others; see Section 1 for an overview of the health data ecosystem).

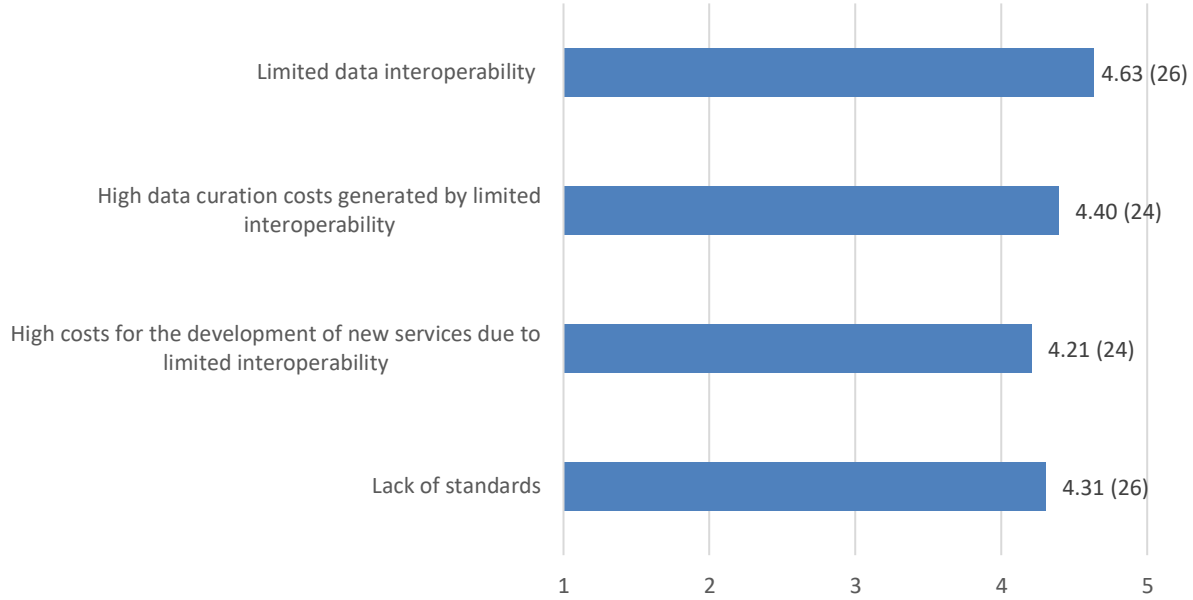
Limited interoperability leads to **high curation costs**, i.e. costs related to the preparation of data for interoperability and sharing. This task can take more than 50% of the time of data scientists working in data sharing projects.[708] Merging different datasets is one of the most resource-intensive activities for data users since datasets are rarely interoperable by default.[709] The high curation costs are indeed a recurring challenge, as confirmed also by the stakeholders consulted for this Study (see Figure 78). In addition, the consulted stakeholders also indicated that limited data interoperability also generates **high costs for the development of new services**, as data needs to be repurposed for the requirements of new projects.

[707] See note 705, p. 1

[708] Everis Benelux (2018) for the European Commission, Study on data sharing between companies in Europe: Final report, p. 27. Available at: https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en

[709] Deloitte (2017) for the European Commission, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, p. 89. Available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51485

Figure 78 Extent to which interoperability-related factors represent barriers to the provision of data-based health services in the EU (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5(to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

Limited interoperability in the field of digital health is a widely acknowledged issue in the EU, mentioned in a series of Commission Communications, such as the eHealth Action Plan 2012-2020[710], the 2018 Communication on eHealth, [711] as well as the 2020 Communication on a European strategy for data.[712] In a public consultation launched by the Commission in 2017 concerning health and care in the Digital Single Market,[713] the consulted stakeholders have stressed the **need for standardisation in the field of health** across the EU. The public consultation also revealed that the main needs stressed by respondents for enhancing health data sharing in the EU revolve mainly around **interoperability issues**. These needs include:[714]

- Standardising Electronic Health Records;

[710] European Commission (2012), Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century, (COM/2012/0736 final). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0736

[711] European Commission (2018), Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, (COM(2018) 233 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A233%3AFIN

[712] See note 80.

[713] College of Europe (2018), Synopsis report of the public consultation on Digital transformation of health and care in the context of the Digital Single Market. Available at: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-digital-transformation-health-and-care-context-digital

[714] Ibid.

- Developing standards for data quality and reliability;
- Introducing cybersecurity standards for health-related data; and
- Adopting open exchange formats to support cross-border interoperability.

It must be noted that, given the importance of the issues, the Commission adopted in 2019 the Recommendation on a European electronic health record (EHR) exchange format, aiming to **facilitate the exchange of specific clinical data**, namely patient summary, ePrescription/eDispensation, laboratory results, medical imaging and reports, hospital discharge reports.[715] The Recommendation outlines principles that should govern the **cross-border exchanges of EHR**,[716] common technical specifications to facilitate the exchanges, as well as a framework for future work to be done in the field.

More generally, the European Commission expert group on FAIR (findable, accessible, interoperable and reusable) data called for the application of the **FAIR principles** to health data to accelerate research, engage the power of new technologies and give data greater value.[717]

6.2 Standards

Arguably the most challenging level of interoperability for the field of healthcare is semantic interoperability. Throughout the existing evidence and feedback from stakeholders, a number of issues are recurrent, such as large amounts of unstructured data, the need for specific data formats, standards for EHR, vocabularies and common terminologies. In this field, the problem is not a lack of standards, but a **lack of *common* standards**. The consulted stakeholders emphasised that standardisation is a significant issue (see Figure 78) and it has more to do with **cooperation and stakeholders agreeing to use the same standards**, rather than working separately and developing different technical specifications and standards that hinder interoperability. Importantly, common standards can also **create more opportunities for SMEs** by enabling better access to the market, as well as reducing technical barriers and costs.[718]

A harmonised approach is essential for enabling cross-border health data sharing in the EU, as well as for building EU-wide health data marketplaces and unified diabetes-related datasets. Several newer developments are encouraging. For instance, the Commission adopted in February 2019 the **Recommendation on a European EHR exchange format**, to support cross-border interoperability for the efficient provision of healthcare in

[715] European Commission (2019), Commission Recommendation of 6.2.2019 on a European Electronic Health Record exchange format, (C(2019) 800 final). Available at: https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

[716] The principles listed in the Annex to the Recommendation are: citizen-centricity, machine readability, data protection and confidentiality, explicit consent or any other lawful basis, auditability, security, identification and authentication of all parties involved in the exchanges, and continuity of service by promptly addressing issues that appear in the system. See: European Commission (2019), Annex to the Commission Recommendation on a European Electronic Health Record exchange format, (C(2019) 800 final). Available at: https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

[717] European Commission Expert Group on FAIR DATA (2018) for the European Commission, Turning FAIR into reality. Available at: https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf

[718] Horgan, D., van Kranen, H.J. & Morré, S.A. (2018), Optimising SME Potential in Modern Healthcare Systems: Challenges, Opportunities and Policy Recommendations, Public Health Genomics, Vol. 21, pp. 1-17. Available at: doi: https://doi.org/10.1159/000492809

the EU.[719] The medical technology industry welcomed this step towards common standards for EHR in the EU and called on stakeholders in the healthcare sector (such as national and regional authorities, providers, industry, etc.), as well as connected sectors (such as providers of consumer devices for lifestyle and well-being, IT, and social media companies, etc.) to **support and adopt common standards** in order to bolster the benefits of an interoperable health data ecosystem.[720] The call also raised an important point about the **need for investment in digital infrastructure** to turn the goal of common standards for digital health into reality. At the EU level, such investments are facilitated by different programmes. For instance, **Horizon 2020** provides funding for research and innovation related to digital healthcare.[721] Specifically for supporting the development of the relevant infrastructure, the **Connecting Europe Facility** provides funding for the deployment of digital infrastructure facilitating the cross-border exchange of health data.[722] More generally, the European Commission supports the digitalisation of public administrations and promotes interoperability of data through the **European Interoperability Framework**,[723] laying out principles and recommendations to improve the interoperability of public services, and the **ISA² programme**,[724] which develops interoperable solutions for public services.

Internationally, standards such as FHIR (Fast Healthcare Interoperability Resources) and openEHR are used to **describe and exchange healthcare data electronically**.[725] FHIR, in particular, appears to have grown in popularity in the past five years, based on the number of mentions in scientific publications.[726] The 2019 report of the Strategic Forum for Important Projects of Common European Interest on "Strengthening Strategic Value Chains for a future-ready EU Industry" emphasises the role of **open international standards in healthcare**. The report recommends establishing "protocols to standardise measurement conditions before data is acquired/measured (sample preparation,

[719] See note 715.

[720] MedTech Europe (2019), MedTech Europe's call to action for an interoperable data ecosystem for digital health. Position Paper, Available at: https://www.medtecheurope.org/wp-content/uploads/2019/07/2019_MTE_DH_Interoperability_position_paper_ws.pdf

[721] See for instance: "DigitalHealthEurope: get support for your digital transformation of health and care activities", published on 19 February 2019. Available at: https://ec.europa.eu/digital-single-market/en/news/digitalhealtheurope-get-support-your-digital-transformation-health-and-care-activities. Last accessed: 20 May 2020.

[722] See for instance: "2019 Connecting Europe Facility (CEF) funding available to foster the deployment of digital infrastructures for the cross border exchange of health data in Europe", https://ec.europa.eu/health/sites/health/files/ehealth/docs/2019_cef_call_en.pdf. Last accessed: 20 May 2020.

[723] European Commission (2017), Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, European Interoperability Framework – Implementation Strategy, (COM(2017) 134 final). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017DC0134

[724] See: "ISA² - Interoperability solutions for public administrations, businesses and citizens", https://ec.europa.eu/isa2/isa2_en

[725] See note 705, p. 2.

[726] Lehne, M., Luijten, S., Vom Felde Genannt Imbusch, P. & Thun, S. (2019), The Use of FHIR in Digital Health - A Review of the Scientific Literature, Studies in Health Technology and Informatics, Vol. 267, pp. 52-58. Available at: https://doi.org/10.3233/shti190805

patient/citizen environment and activity)". For smart medical devices, it suggests considering open international standards (such as IEEE 11073, ITU-T H.810, HL7 FHIR).[727]

Beyond the semantics of health data, **common standards are also needed more widely for medical terms**. The difficulty lies in the variety of natural language and its ever-evolving nature. There are initiatives for standardisation in this area, such as the Systematised Nomenclature of Medicine -- Clinical Terms (SNOMED CT) vocabulary, "the most comprehensive, multilingual healthcare terminology in the world".[728] Such a vocabulary can be used as a basis, updated and complemented with more field-specific terms and concepts.[729]

Nevertheless, there are still issues that prevent the uptake of common standards at the moment. For instance, the European Trade Association representing the medical imaging, health ICT and electromedical industries (COCIR) notes that **developments in the Member States are slow** when it comes to deploying interoperable health solutions.[730] With regard to electronic health records, there is still fragmentation even at the national level, with EU Member States being at different levels of implementation.[731] In addition, while the Recommendation of the Commission on a European EHR exchange format has generally been welcomed by stakeholders in the industry, the question still remains of how effective a **soft law approach** is for driving developments in the field and contributing to a common standard to which all Member States adhere.

The challenge is thus to **ensure cooperation between different stakeholders** leading to the uptake of common standards. The work, however, does not stop there. As the field of digital health is continually evolving, agreeing on a given set of standards at a given point in time will likely not be enough. The solution would rather be a '**living and dynamic standard**', or a 'living dictionary' that captures also the liveliness of the field: new terms and developments should be incorporated and outdated ones discarded in a flexible and rapid manner to **keep up with innovation in the field**.[732]

To ease cooperation, **awareness is also necessary** and scientific projects emphasising the need for interoperability can help. For instance, the **GO FAIR initiative**, a bottom-up and stakeholder-driven initiative, advocates for FAIR data by building networks of stakeholders, offering training on proper data management, as well as designing best

[727] Strategic Forum for Important Projects of Common European Interest (2019), Strengthening Strategic Value Chains for a future-ready EU Industry, p. 48. Available at: https://ec.europa.eu/docsroom/documents/37824

[728] See: SNOMED International (n.d.), 5-Step Briefing. Available at: http://www.snomed.org/snomed-ct/five-step-briefing. Last accessed: 21 May 2020.

[729] See note 705.

[730] COCIR (2019), European Commission's adoption of the recommendation on a European EHR exchange format is welcome. Available at: https://www.cocir.org/media-centre/press-releases/article/european-commission-s-adoption-of-the-recommendation-on-a-european-ehr-exchange-format-is-welcome.html. Last accessed: 21 May 2020.

[731] See note 718. See also: De Raeve, P. (2019), The world of cloud-based services: storing health data in the cloud. Health Europa. Available at: https://www.healtheuropa.eu/cloud-based-services-storing-health-data-in-the-cloud/93053/. Last accessed: 21 May 2020.

[732] See note 596, p. 96.

practices and supporting adherence to existing standards.[733] Increasing the salience of such issues may help to **bring interoperability and common standards higher up on policy agendas** and help drive change.

[733] GO FAIR (n.d.), GO FAIR Initiative. Available at: https://www.go-fair.org/go-fair-initiative/. Last accessed: 22 May 2020.

7. Strategic barriers

Companies that intend to enter the market for data-based health services may face two types of barriers. First, **structural (or natural) barriers may be present in the market**. Such barriers are inherent to the digital economy (such as network effects[734] or economies of scale[735]) and may give a competitive advantage to first movers that are able to build and rely on a sizeable installed customer base. While these barriers cannot be lifted, they should be taken into account and mitigated when designing any policy or rule affecting this market.[736] Second, **strategic barriers may arise**, which can be intentionally created by existing market players to deter entry.[737] In the market for data-based health services, strategic barriers may be raised by parties holding data that are necessary to provide a certain service. These barriers could materialise in several ways such as:

- Charging different prices to different service providers to access the same data;
- Setting prices to access data that are too high and do not allow the provision of competitive data-based health services;
- Refusing requests to access data;
- Allowing consumers to purchase data-based health services only from authorised providers, or offering consumers free/discounted access to data-based health services from authorised service providers; and
- Making access to data conditional to the purchase of other products (e.g. an entire database rather than the specific datapoints needed) or services (e.g. data processing or data curation) sold by the data provider.

Strategic barriers are not necessarily anti-competitive, but can be part of the business strategy of any company that tries to create and maintain a competitive advantage over its peers. When put in place by a player in a dominant position,[738] however, strategic barriers may **impinge on the development of a competitive market for data-based healthcare services**. In this respect, while data providers could seek to control/restrict access to data, **EU competition law** prevents that such restrictions harm the functioning of the market. Competition law may intervene where data providers which are in a

[734] Network effects arise when the value of a given service increases with the number of users of such service.

[735] Economies of scale consist of reductions in the costs of providing services when the scale of operation (i.e. the number of users) increases.

[736] European Parliament Research Service (2020), Is data the new oil? Competition issues in the digital economy, European Union. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf

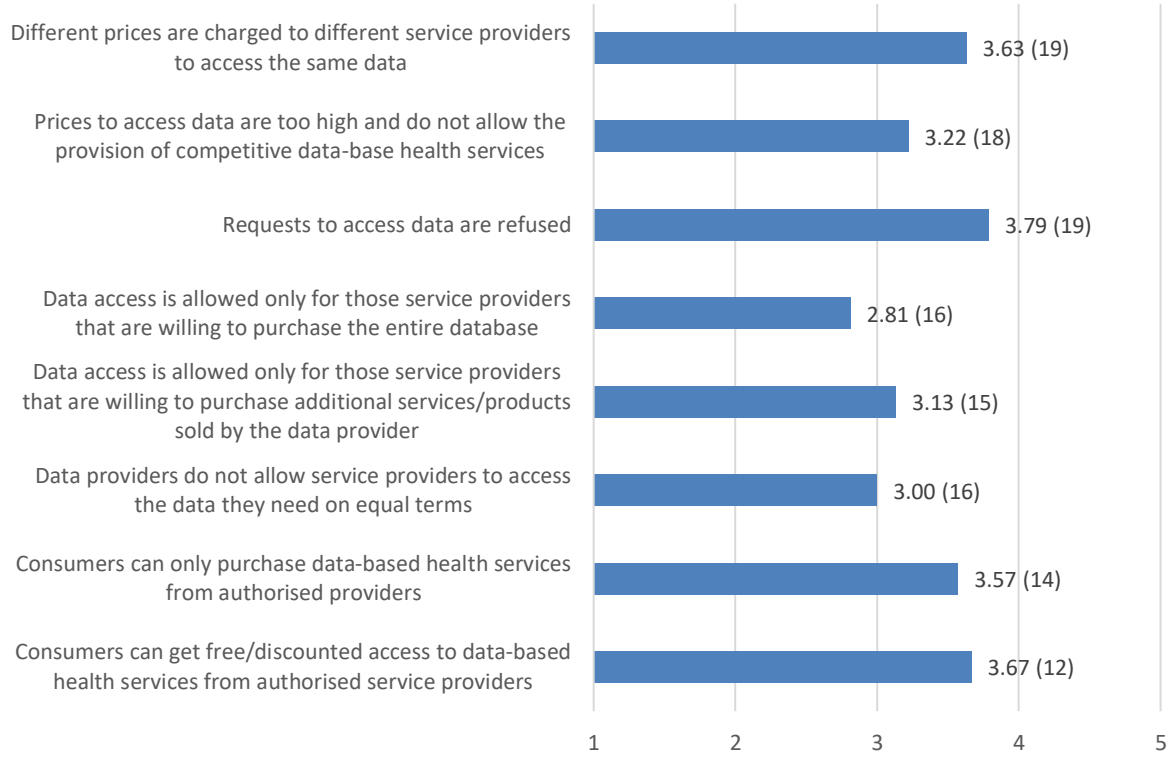
[737] OECD (2007), Competition and barriers to entry, Policy Brief. Available at: https://www.oecd.org/competition/mergers/37921908.pdf

[738] According to the European Court of Justice, a dominant position is "a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of its consumers." (United Brands Company and United Brands Continentaal BV v Commission of the European Communities, Case 2/76). For further details, please see: https://www.concurrences.com/en/glossary/dominance-notion

dominant position attempt to distort the market and hamper the provision of data-based services.

The fact that health data sharing is an **emerging field** has an impact on how strategic barriers have materialised so far. The stakeholders consulted for this Study have generally emphasised that while most of the typical strategic barriers affecting the data economy have not yet materialised in this sector, they may very well occur in the coming future due to the **ever-evolving nature of the field** (see Figure 79). This is particularly true if one considers that a large share of **clinical/medical health data** is concentrated in the national public healthcare systems, and that tech companies are accumulating a sizeable amount of **patient-generated data** (collected via mobile and wearable devices).

Figure 79 Extent to which strategic barriers may limit the development of a competitive market for data-based healthcare services (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' own elaboration on in-depth interviews.

The relevance of strategic barriers and their **implications for the current market and a potential EU-wide health data marketplace**, as emphasised by the feedback from stakeholders and the existing evidence, are discussed in what follows.

Price discrimination

The stakeholders consulted for this Study explained that **differential pricing schemes** for accessing the same health data may apply (see Figure 79). It is worth stressing, however, that this does **not necessarily constitute a barrier to data sharing** in the

field of healthcare. In fact, price discrimination may also generate positive effects.[739] For instance, the consulted stakeholders emphasised that charging relatively lower prices for requests to access data for the purpose of **academic research** may actually foster research activities and lead to positive health outcomes. Differential pricing schemes could also be applied to **support SMEs** that would otherwise not have the necessary means to access the data.

In some cases, however, prices to access data are too high, which could drive out of the market some service providers with more limited financial resources. According to the stakeholders consulted for this Study, the fact that a data provider may set **too high a price to access data** can represent a challenge in the market (at least to some extent), with some categories being potentially more affected than others. In particular, such practices may have a **negative impact on SMEs** who would be looking to compete in the market, but would face difficulties in developing data-driven services in the absence of sufficient funding for accessing the necessary health data. The more data are 'essential' to provide a certain service, the more significant the **data provider's ability to charge a 'premium' price** will be.

These considerations concerning price discrimination are very much linked to the **structure and governance of a potential EU-wide health data marketplace**. As such, differential pricing schemes may hold advantages, by bolstering research and innovation, while also supporting more competition in the market through the presence of SMEs. In this context it is central, however, to set **clear and transparent rules** by which different prices would be charged either to different categories of stakeholders active in the market or for different uses of the relevant data.

Refusal to grant access to data

The stakeholders consulted for this Study emphasised that refusals to grant access to data can **hinder to a high extent the development of a competitive market for data-based healthcare services** (see Figure 79).

The instances in which access to data is refused may take different forms and, as such, carry different implications. For instance, by refusing consent, **the data subject can limit access to data**. In a user-centric model in which individuals are empowered to share their data with the service providers of their choice (see Section 0 for a discussion on different ownership models), each individual may well decide to refrain from sharing his/her data with certain providers on a case-by-case basis. Arguably, having the option to decide with whom data are shared is part of the trust framework of such a model and is thus an important component. Lack of user consent may, however, lead only to small-scale instances of refusal to access data.

In the wider framework of research and commercial applications, ethics committees may also play a role, considering the sensitive nature of data. In fact, **refusal to grant access to data may also result from decisions of ethics committees**, as noted by the consulted stakeholders. Ethics committees have long been involved in establishing guidelines for medical research, such as research involving clinical trials, therefore they

[739] The economic theory confirms that, under specific circumstances, price discrimination can increase social welfare. See by way of example: Papandropoulos, P. (2019), How should price discrimination be dealt with by competition authorities?, Concurrences. Available at: https://ec.europa.eu/dgs/competition/economist/concurrences_03_2007.pdf

may also be an important stakeholder in the approval process of new research and commercial applications.

More generally, **delays in sharing data** may also occur, given the value of novel data for research and commercial applications. Evidence from data sharing practices for clinical trials has shown that instances of refusal to grant access to data do occur and/or **data from clinical trials** are made available with significant delays. A study published in 2018 (looking at industry-sponsored clinical trials in the EU and the US) found that in only 15% of the sampled cases the data stemming from clinical trials for medicine were made available two years after the results of the clinical trial were published. The main reasons were rooted in the **data sharing policies** of the companies involved in the trials. In particular, such policies limit data sharing if the trial data are used for ongoing follow-up research or if the treatment for which the clinical trial was run is still in the process of receiving regulatory approval.[740] Another study from 2019, focused on the US market, also showed that industry data sharing policies can be prohibitive and there is **significant scope for improvement to enhance data sharing**.[741]

Conditional access to data

Aside from refusals to grant access to data, providers of data-based services may also encounter issues of conditional access to data, whereby access is granted only if the service provider purchases an entire database rather than the specific data they need, and/or if they purchase additional services or products sold by the data provider. More generally, **access to the same data may not be granted on equal terms** (other than price terms, which are discussed above under 'price discrimination') **to different service providers**. The consulted stakeholders indicated that these cases are not very frequent in the health sector. Familiarising oneself with the processes to access data stored in different databases can be, however, a laborious task. Indeed, further evidence stemming from the experience of researchers attempting to access health data reinforces these points. The difficulties reported by researchers include **different and complex requirements to access datasets** as well as the **requirement to specify upfront the type of data needed**, without having a clear understanding of what may be available in the database.[742]

When it comes to the specific terms based on which different service providers are allowed to access data, the consulted stakeholders also noted that this is not necessarily an issue, as long as the **policies for accessing data are clear and transparent**. In fact, such situations are seen as being rather similar to having a differential pricing system in place.

Distortions of consumer choice

[740] Hopkins, A.M., Rowland, A. & Sorich, M.J. (2018), Data sharing from pharmaceutical industry sponsored clinical studies: audit of data availability, BMC Medicine, Vol. 16, 165. Available at: https://doi.org/10.1186/s12916-018-1154-z

[741] Miller, J., Ross, J.S., Wilenzick, M. & Mello, M.M. (2019), Sharing of clinical trial data and results reporting practices among large pharmaceutical companies: cross sectional descriptive study and pilot of a tool to improve company practices, BMJ, Vol. 366 :l4217. Available at: https://doi.org/10.1136/bmj.l4217

[742] Butler, B. (2020), The researchers' experience when attempting to access health data for research, National Cancer Research Institute. Available at: https://www.ncri.org.uk/ncri-blog/accessing-health-data-for-research/. Last accessed: 22 May 2020.

Strategic barriers can also occur when **the consumers' choice of data-based services is influenced** through practices such as allowing consumers to purchase data-based health services only from 'authorised' providers, or offering consumers free or discounted access to services from 'authorised' providers. The stakeholders consulted for this Study confirmed that such situations may occur in the market (at least to some extent); nevertheless, this is in general not seen as a barrier to the development of a competitive market for data-based healthcare services. In particular, stakeholders stressed that in **public healthcare systems**, which are prevalent in the EU, such barriers may, in fact, be put in place by the national healthcare system to exclude, for instance, low-quality services. In this case the narrative would change: authorisation would thus not be a barrier *per se*, but rather a **protective measure for patients and consumers in general**. Rules for authorisation should be, however, scrutinised to ascertain that they do not create unnecessary barriers to entry or favour some players over others.

Another situation in which a service provider may need prior authorisation could be in the emerging field of **data intermediation platforms** that allow users to organise their data and share it with service providers on the platform. In this case, the services available for consumers to choose from may be subject to **prior authorisation from the data intermediary**. Such processes should be, however, governed by **clear and transparent rules of the platform** and applied in the same way to all service providers interested in offering their services through the platform. In-depth scrutiny of relevant terms and conditions may well be needed in all cases where such platforms hold a dominant position.

An EU-wide B2B health data marketplace should take such issues into consideration. A potential **authorisation process for data providers** could take different forms depending on the entity supposed to provide such authorisation, for instance, public authorities or private data intermediaries. Regardless of the authorising entity, a **transparent and non-discriminatory** process should be ensured to **avoid unnecessary barriers to entry, especially for SMEs**, while mitigating any safety and security risks.

Other strategic barriers

Strategic barriers may also be linked to **interoperability**. For instance, to maintain a competitive advantage, a stakeholder or a group of stakeholders could develop proprietary standards, creating data ecosystems around them. This, in turn, would make it difficult for other stakeholders in the market, who rely on different standards for their processes, to access the newly created data ecosystem. Such a situation would result in an **indirect barrier to data sharing** due to the limited interoperability. In addition, the choice of what specifications become standards at the market level can create a barrier to entry when the chosen specifications clearly favour some market players over others, resulting in the lockout of some providers from the market.

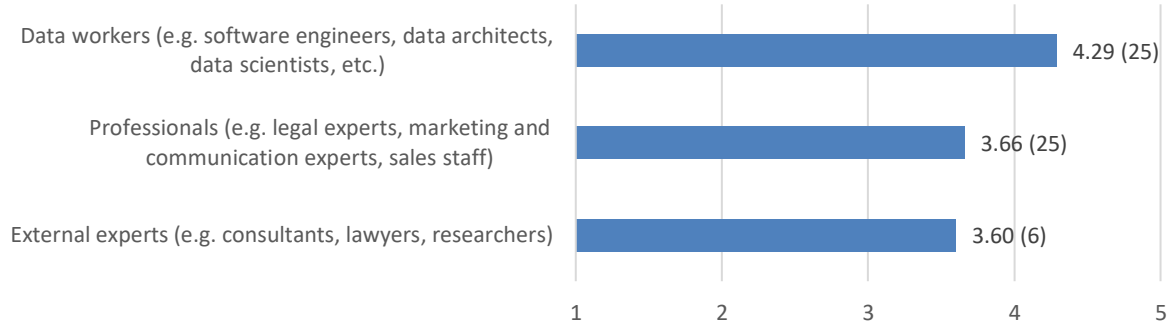
8. Other barriers

8.1 Knowledge and skills

The lack of data knowledge and skills creates a **barrier for companies to adopt data sharing practices**. According to a survey carried out by Everis Benelux in 2018,[743] four out of ten companies highlight the lack of data knowledge and skills as a relevant obstacle to data sharing in the EU. Not only **data workers** (such as software engineers, Geographic Information Systems analyst, data architects, data scientists and developers) are needed as the digital economy develops, but also other job profiles such as **legal experts**, **marketing**, **communication and sales staff**. Due to the shortage of skills, companies lose time or miss business opportunities as data are not used to their full potential. To compensate for this shortage, many companies resort to support from **external partners** (e.g. universities or established software, electronics and technology suppliers such as Intel, Pioneer, DJI, NVidia or Oracle).

Skill gaps are also materialising in **the field of digital health**. The stakeholders consulted for this Study emphasised the lack of professionals across a range of domains (see Figure 80). In particular, the most stringent need in the digital economy is for **data workers with field-specific expertise**. Given the importance of standards, terminologies and ontologies in the field of healthcare, stakeholders emphasised the need for highly trained data scientists, developers and software engineers who also understand and can navigate the intricate landscape of medical health.

Figure 80 Extent to which limited data knowledge and skills may create barriers for companies to provide data-based health services in the EU (average score of answers, number of respondents)



Note: The results are not statistically representative; Likert scale: from 1 (not at all) to 5 (to the fullest extent).
Source: Authors' elaboration on in-depth interviews.

At the same time, there is also a need to ensure that healthcare professionals have the necessary digital skills to foster the uptake of digital health solutions. In a statement from 2019, the European Medical Students' Association stressed the need for updated curricula featuring **digital skills for healthcare professionals** as well as exchanges of best

[743] Everis Benelux (2018) for the European Commission, Study on data sharing between companies in Europe: Final report, p. 77. Available at: https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en

practices when it comes to digital health in medical education.[744] Training in digital skills should not be limited to medical school curricula, but should also become part of a wider strategy for **life-long learning**, enabling healthcare professionals to make the best use of emerging data-based therapies.[745]

In addition, given the potential applications based on patient-centric care and patient empowerment with regards to data sharing, there is also a **need to train patients** as much as health professionals to ensure that they can effectively use new data-driven technologies for healthcare.[746] More generally, increasing **digital literacy skills among individuals** could also facilitate the uptake of digital health solutions.[747]

Other professionals (such as legal experts, marketing and communication experts, sales staff) and external experts (including consultants, lawyers, researchers) who are able to provide **guidance for the provision of data-based health services** are also considered important, but to a lesser extent in comparison to data workers with expertise in the field of healthcare.

In addition, the consulted stakeholders indicated that **new job profiles** could emerge to support the development of the digital health industry. Such job profiles would play an important role in helping stakeholders better understand the developments in the field of digital health and enable them to optimise their decisions. In this respect, the following profiles would be relevant:

- **Health data officer**: As digital health is a complex and broad field, bringing together both medical skills and skills from the realm of data science and policy becomes essential. Professionals who are able to ensure the link between the different spheres could be beneficial in the ecosystem. Just as the GDPR instated a new position, that of data protection officer, organisations could rely more generally on 'health data officers', who would operate **at the intersection between the medical and the data world**, and would have an understanding of both the medical environment and data-related developments; and
- **Data coach/consultant**: In a similar vein, patients and individuals in general could benefit from **assistance in understanding the advantages and disadvantages of digital health solutions** for their specific situations. In this respect, a data coach or consultant could help individuals understand the full potential of their data, what solutions are available, and what implications each of them carries with respect to e.g. privacy, security, etc.

[744] European Medical Students' Association (2019), Digital Health in the Medical Curriculum: Addressing the Needs of the Future Health Workforce. Available at: https://emsa-europe.eu/wp-content/uploads/2019/09/Digital-Health-in-the-Medical-Curriculum_-Addressing-the-Needs-of-the-Future-Health-Workforce.pdf. Last accessed: 22 May 2020.

[745] European Health Parliament (2016), Committee on Digital Skills for Health Professionals, Digital Skills for Health Professionals, p. 6. Available at: https://www.healthparliament.eu/wp-content/uploads/2017/09/Digital-skills-for-health-professionals.pdf. Last accessed: 22 May 2020.

[746] See note 590, p. 327.

[747] BEUC (2018), Digital Health: Principles and Recommendations. Available at: http://www.beuc.eu/publications/beuc-x-2018-090_digital_health_-_principles_and_recommendations.pdf, pp. 20-21. Last accessed: 22 May 2020.

8.2 Financial barriers for SMEs

Faced with the outbreak of the COVID-19 pandemic, the problem of **access to financing** is of greater concern to SMEs in 2020 than in previous years. Indeed, according to the Survey on the Access to Finance of Enterprises, 10% of the surveyed SMEs stated that access to finance is one of their main concerns.[748] In particular, a study carried out by the European Commission[749] explains that while **bank loans traditionally represent the main source of funding for SMEs** in all EU countries, "access to bank financing is much more difficult for innovative, smaller and younger SMEs". These entities often lack collateral and equity as well as a well-established relationship with financial institutions.

Loan availability, however, hides important discrepancies at the Member State level. Due to the variety of the banking landscape across Europe, SMEs experience more difficulties in accessing bank financing in countries such as Ireland, Estonia or the Netherlands, where a few large banks account for more than 80% of the market share, resulting in less favourable financing conditions than in Austria, Denmark, France or Germany, where the high number of banks makes it possible to further support the local economy with better financing conditions.

At the same time, the shortage of transversal skills (see also the discussion on skills and knowledge Section 0) may also result in SMEs being **less aware of financial opportunities** that may be available to them. A study conducted by CEPS[750] points out that the complex financing landscape can be a hurdle as well. In particular, the far too wide variety of funds to finance innovative SMEs is likely to increase management and administrative costs, while also making it difficult for SMEs to access funding given the effort and knowledge necessary to navigate this complex landscape.

Beyond the need for funds, other factors can turn out to be rapidly onerous and can dissuade SMEs from engaging in data exchange models or force them to exit the market:[751]

- **Infrastructure and facilities.** Providing support for the development of a sufficient level of infrastructure (for instance, ICT facilities, laboratories, and even legal support) would enable innovative SMEs to perform testing of real-life prototypes. In the field of data economy, infrastructure support could inter alia feed into the development of solid data protection systems. By focusing on this issue, the government would support the development of innovative SMEs and, more generally, boost innovation and the cutting-edge technology. In addition, solid infrastructure would enhance confidence from users/stakeholders (see Section 0);

[748] SME access to finance conditions, 2020 SAFE details - European Union. Available at: https://ec.europa.eu/docsroom/documents/43869

[749] European Commission (2019), SME Envoys Finance SME access to finance situation in EU Member States Final Report 2019, p.4. Available at: https://ec.europa.eu/docsroom/documents/39645

[750] CEPS (2019), Hidden Treasures - Mapping Europe's sources of competitive advantage in doing business, p.15, p.83-84, p.98-100. Available at: https://www.ceps.eu/ceps-publications/hidden-treasures/

[751] Ibid.

- **A more SME-friendly patent system.** Two studies from the European Patent Office (2019)[752] and European Union Intellectual Property Office (2019)[753] show that SMEs that have engaged in Intellectual Property Right activities tend to grow at a faster pace than other SMEs. A trend that is even more prominent for high-tech SMEs. However, in many Member States oligopolies among commercial patent lawyers have been formed, increasing the costs for SMEs; and
- **Access to justice**. SMEs often lack the resources to sustain litigation over a long period of time. As highlighted in Section 7, strategic barriers may arise in the field that could not only limit the opportunities for SMEs to gain access to the market and to consumers but that could also lead to considerable legal costs for SMEs, especially in the area of open innovation where creative SMEs may not have sufficient bargaining power against large firms. Such costs could drive some SMEs out of the market.

[752] European Patent Office (2019), Annual Report of the Board of Appeals and European Patent Office. Available at: https://www.epo.org/law-practice/case-law-appeals/annual-report.html

[753] European Union Intellectual Property Office (2019), High-growth firms and intellectual property rights IPR profile of high-potential SMEs in Europe, May 2019. Available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_High-growth_firms_and_intellectual_property_rights/2019_High-growth_firms_and_intellectual_property_rights.pdf

9. Policy recommendations

Data-driven services and data sharing for research present a **unique opportunity to improve healthcare outcomes in the EU**. To unlock the full potential of health and well-being data – from the traditional data collected in health records to emerging biomarkers recorded through smartphones – a data-sharing framework supported by all stakeholders and rooted in trust is needed.

The barriers to health data sharing, described throughout this Study, can be overcome. In a nutshell, the **actual and potential barriers** identified are: i) the requirements applicable across the EU for the protection of personal data and health data in particular; ii) the uncertainty around who is held liable in case of damages stemming from data-driven services and how the quality of the data should be ensured in a marketplace; iii) the need for accountability and trust for sustaining a data-sharing framework; iv) the need to ensure that data can flow seamlessly, supported by interoperable and standardised systems and processes; v) the potential strategic barriers to accessing data; and vi) the need for digital literacy and skills.

The opportunities presented by data sharing and health data marketplaces can be bolstered and brought to fruition with the **right governance framework**. This concluding Section puts forward policy recommendations in support of such a framework, with **trust as the common and clear thread** underpinning it.

Reducing the costs of data sharing

Ensuring harmonised implementation of data protection rules. The GDPR plays a central role in fostering trust and introducing a level playing field for data protection across the EU. Nevertheless, differences can arise due to the way in which the Regulation is applied at the Member State level. In particular, such differences can stem from the fact that health data are considered sensitive data under the GDPR, allowing Member States to introduce more stringent provisions as they deem necessary. However, for businesses seeking to operate cross-border – particularly SMEs, such differences can be hurdles and translate into compliance burdens. To achieve EU-wide B2B health data marketplaces, the EU should oversee the implementation of data protection rules, continue to provide guidelines through the EDPB and foster coordination for harmonised legislation in all Member States.

Limiting fragmentation due to diverging national rules. Fragmentation is likely to occur especially if one considers that health law is not harmonised across the EU, and neither is contract law, beyond the existence of guidelines issued by the Commission on specific issues, such as the sharing of private-sector data.[754] To mitigate such issues, the Commission can play a coordinating role, monitoring how liability rules, particularly in the field of digital health, evolve in the Member States and should also promote a coherent approach to facilitate cross-border data exchanges.

Developing guidelines for anonymisation techniques compliant with the GDPR. While anonymised data are not subject to the GDPR as they do not involve personal data, significant uncertainty remains about what is considered anonymised data and what anonymisation techniques should be employed to ensure that once such techniques are

[754] European Commission (2018), Commission Staff Working Document. Guidance on sharing private sector data in the European data economy, (SWD(2018) 125 final). Available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy

applied, the resulting data can be considered anonymous for the purposes of the GDPR. Different anonymisation techniques do exist, but specific guidance on their application and the accompanying regulatory implications is lacking. Against this backdrop, guidelines for anonymising data should be developed considering the variety of applications that health data can have for the development of innovative services, such as the provision of personalised treatment within a medical context, the development of data-based services such as lifestyle apps, and research.

Fostering cooperation for common standards. The technical solutions enabling data exchanges are the backbone of effective health data sharing and B2B health data marketplaces. Cooperation is essential to ensure the uptake of standards and technical specifications. In particular, at the EU level, the impact of the Recommendation on a European EHR exchange format[755] should be closely monitored to determine the extent to which the provisions on standards were adopted by Member States. More widely, continued cooperation concerning standards in the field of digital health should be promoted. As the field is continuously evolving, agreeing on a given set of standards at a given point in time will likely not be sufficient. The solution will rather be a 'living and dynamic standard', or 'living dictionary' that would also capture the liveliness of the field: new terms and developments should be incorporated and outdated ones should be discarded in a flexible and rapid manner to keep up with innovation in the field. This possibility could be explored to enable innovation that is not hindered by the slow development and uptake of standards.

Increasing user trust

Defining a framework for responsibility for the quality of data. Different stakeholders – such as the data providers, the owners of a potential B2B health data marketplace, and the providers of data-based services – play an important role in ensuring the quality of the data that is shared in the EU-wide B2B marketplace. Low-quality data may lead to services of equally poor quality, which may result in damages. For the well-functioning of a marketplace, it would thus be important to define a framework establishing who is liable for the quality of data shared and used. Such a framework would most likely need to acknowledge the chain of responsibility when data are shared: the data providers would be responsible for the data made available on the market, the providers of services would be responsible for any issues resulting from their processing of such data, while the owners of the marketplace would be responsible for the general governance of the marketplace, for setting rules and overseeing how stakeholders in the market abide by them. The ultimate goal of such a framework should be to establish clear rules on liability stemming from the low quality of data. This would reduce uncertainty for businesses and litigation costs, provide incentives to improve data quality, and ultimately increase consumers' trust.

Updating liability rules to meet the challenges of digital transformation. With the proliferation of new digital technologies and services, the EU liability framework, which is largely based on the Product Liability Directive,[756] is put to the test. A potential revision of the Directive should take into consideration the challenges posed by the digital era,[757]

[755] See note 715.

[756] See note 663.

[757] Expert Group on Liability and New Technologies - New Technologies Formation (2019), Liability for artificial intelligence and other emerging digital technologies, European Commission, pp. 27-28. Available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

particularly to provide for a liability framework for services based on healthcare data and those applications that do not fall directly under the scope of the Medical Device Regulation.

Establishing accountability mechanisms for increased transparency. To gain the trust of individuals in data sharing, it is important to mitigate their concerns about what happens to their data, who has access to them, how they are protected, who is responsible for data privacy breaches and who one can appeal to in case problems arise. Businesses wishing to engage in health data sharing should be prepared to provide clear and concise answers to such questions coming from consumers. In this regard, accountability mechanisms for stakeholders sharing and using health data should consist of internal control systems that produce evidence such as audit reports, which can be presented not only to data subjects (consumers) but also to supervisory bodies and other stakeholders. For effective communication, the information provided to consumers, or individuals more generally, should be as clear and concise as possible, giving straight answers to questions rather than overflowing individuals with information. Such a forthcoming approach can help to address initial privacy and security concerns, mitigating the fear of data misappropriation and the uncertainties about what can be done with the data.[758]

Setting up feedback loops for the sustained engagement of individuals in data sharing. Particularly in a research setting, a feedback loop, providing information to the participants about the research results, could enhance transparency. This can build more trust and generate more involvement and engagement of individuals throughout the research process.

Creating a 'privacy label' for apps. To increase transparency and address potential concerns around data privacy and security, introducing a 'privacy label' for health apps should be considered. Such a label could contain information about the underlying technology and the level of privacy of the application in a clear and distilled fashion, similar to nutrition labels. In addition, a privacy label can be a self-regulatory measure, allowing developers to distinguish themselves by the importance they place on the security and privacy of the user data that is shared through the app.

Fostering competition and innovation

Further enabling data portability through technical requirements. The right to data portability as inscribed in the GDPR has opened the possibility for more user-centric and user-driven data sharing.[759] However, the right of the user to receive their data does not necessarily mean that the data can be easily reused for other services. The review of the GDPR should consider bolstering this legal provision with a technical provision that specifies the technical means through which access to data is granted. In this case, APIs[760] could be the technical tool to enable easier access to data.

[758] Such issues are mentioned in the communication from the Commission on a European strategy for data. See note 80, p. 7.

[759] Ibid., p. 10.

[760] APIs are a technical solution that supports the interoperability of a given system or application by providing an interface through which other systems and applications can link, facilitating data exchanges. See for instance: Article 29 Working Party (2016), Guidelines on the right to data portability, p. 5. Available at: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Fostering interoperability to avoid indirect restrictions to accessing data. A lack of interoperability, resulting from the decision of some market stakeholders to follow their own specifications for their services, may lead to lock-in effects. Promoting the use of common standards and specifications is essential to unlock the potential of Big Data and to ensure that a competitive market allowing for data sharing and reuse is in place.

Developing an EU framework for the secondary use of health data.[761] Uncertainty around data anonymisation is also linked to the secondary use of health data, for applications such as research and wider public health considerations. With the rise of Big Data, the opportunities in this field can be significant and a clear EU framework for using health data in such contexts could open up new opportunities.[762] The Finnish national law on the secondary use of health data[763] is an example of policy action that supports legitimate developments in this field. Introducing a framework for the secondary use of health data at the EU level, building on the example of the Finnish law in this field, could encourage research and innovative data-based applications. An EU framework for the secondary use of health data can thus be a building block to establish EU-wide (B2B) health data marketplaces.

Supporting stakeholders in accessing the market. Accessing data may come at costs that are difficult to bear by some stakeholders such as academic and research organisations or SMEs. To support research and innovation, while also encouraging competition through the presence of SMEs in the market, it is important to consider supporting differentiated pricing schemes for data access to enable specific categories of stakeholders (who would otherwise find the pricing prohibitive) to enter the marketplace.

Developing clear and transparent rules for data access. The sensitivity of health data requires a serious reflection on data access rights for different categories of stakeholders active in the market. Data access should allow the development of innovative data-based services within a framework that fosters trust and cooperation. As such, access to specific types of health data for service providers could be made contingent on prior authorisation by, for instance, public authorities.

Making Europeans ready for digital healthcare services

Fostering data literacy skills in healthcare professionals and patients alike. With the growing potential of applications based on patient-centric care and patient empowerment, there is a need to train patients as much as health professionals to ensure that they can effectively use new data-driven technologies for healthcare. More generally, increasing digital literacy skills among individuals could also facilitate the uptake of digital

[761] This recommendation is also echoed in the report of the Strategic Forum for Important Projects of Common European Interest. See: Strategic Forum on Important Projects of Common European Interest (IPCEI) (2019) for the European Commission, Strengthening Strategic Value Chains for a future-ready EU Industry, p. 48.

[762] See the discussion in Section 0 4.2 **Data anonymisation**.

[763] The Act on the Secondary Use of Social and Health Data of 26 April 2019, https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf

health solutions.[764] Targeted training for healthcare professionals, and information campaigns to raise awareness among individuals, made available through, for instance, the websites of public authorities in a format that is easy to understand can help bridge the gap in data literacy skills.

Preparing data workers with field-specific knowledge. Given the importance of standards, terminologies and ontologies in the field of healthcare, there is a stringent need for highly trained data scientists, developers and software engineers who also understand and can navigate the intricate landscape of medical terminologies. Education and training policies should thus be ready to meet this need by updating curricula and encouraging joint specialisations, for instance in data science and health studies.

Supporting the creation of new job profiles acting as facilitators in the digital health ecosystem. The interplay between new digital technologies and healthcare can create a rich ecosystem in which skilled professionals that can navigate both the digital and the healthcare sphere become highly relevant. Supporting the development of new jobs linking the two spheres will result in better outcomes for the stakeholders in the ecosystem. By way of example, just as the GDPR instated the data protection officer position, organisations could rely more generally on 'health data officers', who would operate at the intersection between the medical and the data world, and would have an understanding both of the medical environment and of data-related developments. In the same vein, a data coach or consultant could help patients and individuals understand the full potential of their data, what solutions are available, and what implications in terms privacy and security may stem from relying on such solutions.

[764] BEUC (2018), Digital Health: Principles and Recommendations, pp. 20-21. Available at: http://www.beuc.eu/publications/beuc-x-2018-090_digital_health_-_principles_and_recommendations.pdf. Last accessed: 22 May 2020.