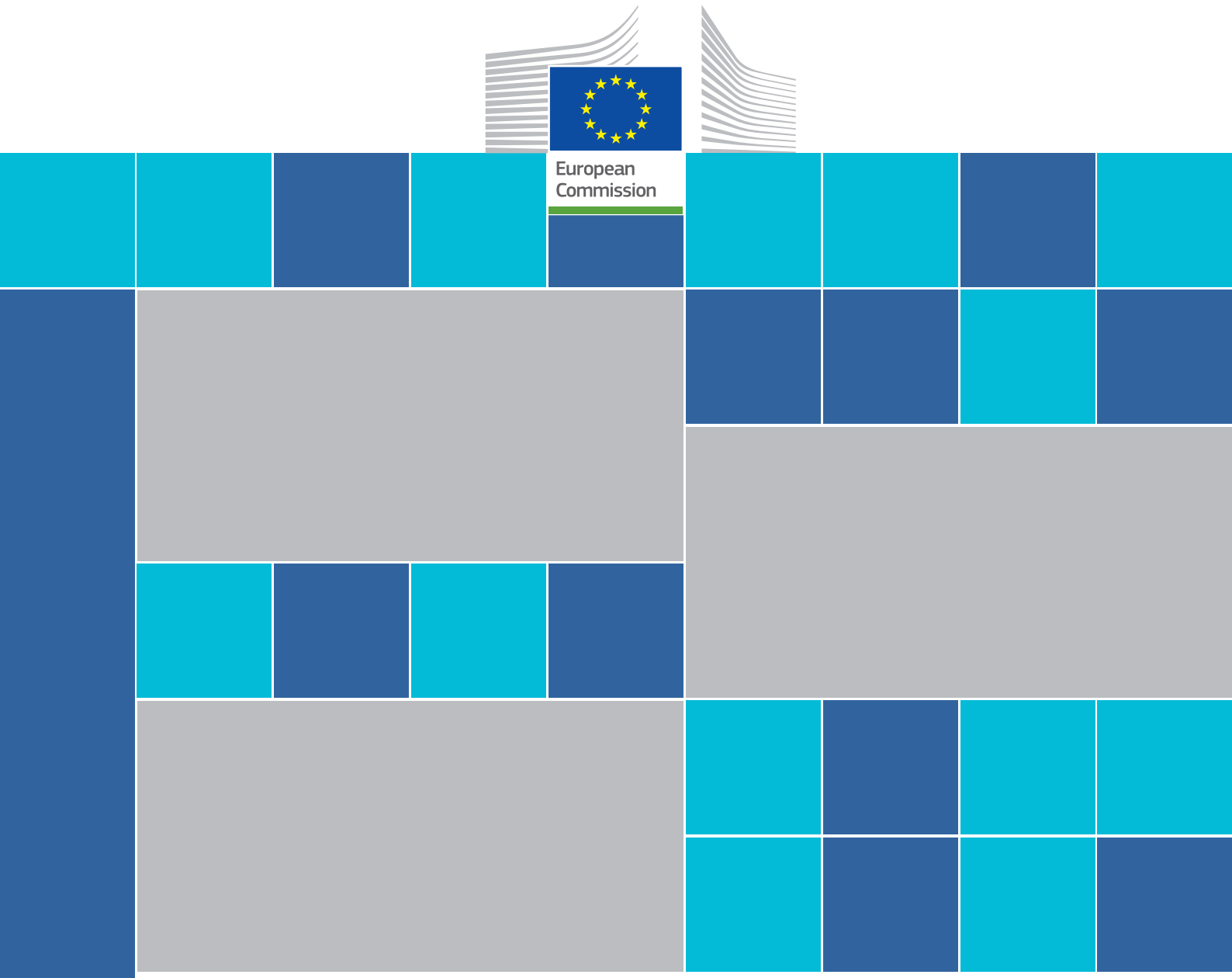


DG Health and
Food Safety

Assessment of the EU Member States' rules on health data in the light of GDPR

Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03

Health and Food Safety

Further information on the Health and Food Safety Directorate-General is available on the internet at: http://ec.europa.eu/dgs/health_food-safety/index_en.htm

Luxembourg: Publications Office of the European Union, 2021

PDF ISBN 978-92-9478-785-9 doi:10.2818/546193 EB-01-21-045-EN-N

Assessment of the EU Member States' rules on health data in the light of GDPR

Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03

Written by Johan Hansen[1], Petra Wilson[2], Eline Verhoeven[1], Madelon Kroneman[1], Mary Kirwan[3], Robert Verheij[1,4], Evert-Ben van Veen[5] (on behalf of the EUHealthSupport consortium)

[1] Nivel, Netherlands institute for health services research, [2] Health Connect Partners, [3] Royal College of Surgeons in Ireland, [4] Tilburg University, [5] MLC Foundation

Contributors:
Peter Achterberg, Jeroen Kusters, Laura Schackmann (main report), Isabelle Andoulsi, Petronille Bogaert, Herman van Oyen, Melissa Van Bossuyt, Beert Vanden Eynde, Marie-Eve Lerat (BE), Martin Mirchev (BG), Radek Halouzka (CZ), Mette Hartlev, Klaus Hoeyer (DK), Fruzsina Molnár-Gábor (DE), Priit Koovit (EE), Olga Tzortzatou, Spyridoula Spatha (EL), Pilar Nicolás, Iñigo de Miguel Beriain, Enrique Bernal Delgado, Ramón Launa (ES), Gauthier Chassang, Emmanuelle Rial-Sebagg (FR), Damir Ivanković, Ivana Pinter (HR), Luca Marelli, Edoardo Priori (IT), George Samoutis, Neophytos Stylianou (CY), Santa Slokenberga, Agnese Gusarova (LV), Laura Miščikienė, Lukas Galkus (LT), László Bencze (HU), Philip Mifsud, Philip Formosa (MT), Dorota Krekora (PL), Alexander Degelsegger-Márquez, Anna Gruböck, Claudia Habl, Kathrin Trunner (AT), Cátia Sousa Pinto, Joana Luís and Diogo Martins (PT), Daniel-Mihail Sandru (RO), Metka Zaletel, Tit Albreht (SI), Peter Kováč (SK), Jarkko Reittu (FI), Lotta Wendel (SE), Edward Dove (UK)

Consumers, Health, Agriculture and Food Executive Agency
Third EU Health Programme

2021 EN

EUROPEAN COMMISSION

Consumers, Health, Agriculture and Food Executive Agency
Unit: Health Unit

Contact: Marilena Di Stasi

E-mail: Marilena.Di-Stasi@ec.europa.eu

European Commission
B-1049 Brussels

CONTENT

Note. Country fiches describing each MS are published as stand-alone report

Abbreviations:

CIDR	Computerized Infectious Disease Reporting System (Ireland)
CRUD	create, read, update and delete
eEHIF	eHealth EU Interoperability Framework
EHR	Electronic health record
ELGA	Austrian EHR system
EMA	European Medicines Agency
FAIR	Findable, Accessible, Interoperable, Reusable
GDPR	General Data Protection Regulation
HCP	Healthcare provider
HDR	Health data research
HTA	Health Technology Assessment
ICT	Information and communication technology
IHR	International Health Regulations (WHO)
MoH	Ministry of Health
MS	Member State(s)
NHS	National Health Services
PHE	Personal Health Environment
PHR	Personal health record
PMS	Post market surveillance
REC	Research Ethics Committee
WHO	World Health Organisation

EXECUTIVE SUMMARY

In the context of the Single Framework Contract Chafea/2018/Health/03 between the EUHealthSupport Consortium and the Consumers, Health and Food Executive Agency (Chafea), a study was conducted with the objective to examine and present the EU Member States' rules governing the processing of health data in light of the GDPR, with the objective of highlighting possible differences and identifying elements that might affect the cross-border exchange of health data in the EU, and examining the potential for EU level action to support health data use and re-use.

We distinguish between using health data for primary purposes (for treatment of the patient) and secondary purposes (for research, registries and management of the healthcare system). The study provides an evidence-based comparison of the state of play regarding health data governance within the EU. This will help to assess in what areas EU intervention might be needed and if so, through which types of measures, be it measures such as a Code of Conduct for data processing in the health area, which could be supported by an EU level implementing act or more direct legislative action, taking into account the particularities of the health systems in the Member States.

The study uses a mixed-methods approach, consisting of the following elements:

- **Literature review** to provide an overview of best practices, bottlenecks, policy options and possible solutions already identified in the literature.
- **Mapping legal and technical aspects of health data usage at national level** to provide an overview of the differences among countries in legislation, regulation and governance models regarding processing health data.
- **In-depth case studies** of national governance models for health data sharing.
- **Workshops** held with MoH representatives, experts, stakeholder representatives and experts from national data protection offices.
- **Stakeholder Survey** to cross validate and supplement the topics addressed and identified in the Member State legal and technical aspects mapping.

The results of this study allow for a detailed assessment of possible elements at Member States/EU level that might affect the movement of health data across borders. It also identifies practices that could facilitate this exchange of data, as well as possible policy options for strategies in this area. Finally, we explored possibilities for sustainable governance structures for health data collection, processing and transfer, as well as measures empowering citizens to have more control of their own health data and to ensure portability and interoperability of these data.

The work conducted in the context of this study makes clear that a number of legal and operational issues need to be addressed to ensure that European healthcare systems can make best possible use of health data for the three interlinked purposes of primary use for direct patient care, secondary use to support the safe and efficient functioning of healthcare systems, and secondary use to drive health research and innovation. It is clear from the views shared in the workshops and by country correspondents to the legal and technical survey that while the GDPR is a much appreciated piece of legislation, variation in interpretation of the law and national level legislation linked to its implementation have led to a fragmented approach which makes cross-border cooperation for care provision, healthcare system administration or research difficult. In view of the margin of manoeuver left to Member States in the GDPR to further specify the application of the Regulation in the area of health and article 168 Treaty on the Functioning of the European Union, a fully harmonised approach to the rules on processing of data in the area of healthcare provision, administration or research across the EU has not been achieved. Furthermore, the interpretation of the law is complex for

researchers at national level and patients do not always find it easy to exercise the rights granted by the GDPR. Taken as a whole, the evidence gathered through the study shows that there is a strong interest in the prospect of a European Health Data Space, but highlights that it would require a sound level of legal and operational governance. The need for operational governance embracing the FAIR data principles[1] was highlighted, which in turn emphasised the need for wide-spread implementation of technical standards to ensure data interoperability and to build trust in data governance amongst EU citizens.

There is a good level of support for actions at EU level to promote health data access and sharing. Such measures may include a combination of soft law (via a Code of Conduct) with other non-legislative and legislative actions. A Code of Conduct is considered desirable to explain concepts from the GDPR and to ensure a consistent approach to health data exchange at a more practical level (e.g. defining formats for data exchange). A challenge for EU legislation is that it should be supportive of the ways health systems are organised in the different Member States. The empirical work identified significant support for the creation of an infrastructure to facilitate data access and sharing, although there is no clear preference with regard to the way such an infrastructure should be set up. There is however a preference to regulate the operation of the infrastructure centrally via an EU agency or EU committee, rather than via a voluntary network. When a structure is set up or a Code of Conduct is drafted, a broad representation of stakeholders is considered important, including organisations engaging into scientific research, regulatory bodies, patients and policy makers.

The topics explored not only address issues concerning legal requirements and governance, but point equally so to technical infrastructure, technical and semantic interoperability, data quality, data acquisition and digital skills and capacity building in the Member States. This also demands the full support to patients to act as active agents in their own health and care, with full capacity to exercise their health data related rights. Taken together these factors can be regarded as pillars of trust that are necessary to enhance the development of a European Health Data Space.

It is clear that addressing health data sharing and governance requires a multifaceted approach. The identified future EU level actions, that should be complementary and cumulative, include stakeholder driven codes of conduct, new targeted and sector specific EU level legislation, guidance and support to the cooperation among Member States and relevant stakeholders, but also support for digitalisation, interoperability and digital infrastructures, allowing for the access to and use of data for healthcare, policy making and research and innovation. It is important that these future actions are developed in full respect of principles of proportionality and subsidiarity.

Whatever next steps are chosen a EU level, it is clear that co-operation between EU Member States is crucial. Such co-operation should draw upon the work of national level data protection authorities coming together as the European Data Protection Board, as well as the numerous national and EU level bodies that represent patients, patients of specific disease groups, healthcare professionals, researchers and industry. The COVID-19 pandemic has done much to increase willingness for such co-operation and provides many new models for rapid, responsive and impactful action.

[1] Findable, accessible, interoperable, reusable

1. INTRODUCTION

1.1. Data for sustainable health care

It is widely acknowledged that safe, efficient and sustainable healthcare systems are highly dependent on data. Data may support clinical decision making, may allow for healthcare system planning, supervision and improvement and may provide information to empower patients to engage actively in their healthcare and wellness management.

Such data includes formally structured data in electronic health records, medical images, drug prescriptions, laboratory reports, claims and reimbursement data, patient reported outcomes and other data management tools used within healthcare systems. It also includes data generated outside the healthcare setting, such as data from wellness devices such as fitness trackers and other data originating from a wide range of settings. Together they form the basis of what has been described as a learning health system (Menear et al 2019; Friedman et al 2016). Principles like data FAIRness (findable, accessible, interoperable and reusable) and value-based health care are intrinsically connected with the concept of learning health systems.

The COVID-19 pandemic has significantly focussed attention on data sharing, both in the context of public health reporting of disease incidence and contact tracing, and in the need for accessible data for collaborative research across many countries; both within and beyond the EU. Furthermore, such data will be needed to evaluate the effects of treatment and vaccines once they become available. The focus on better data availability and accessibility was however already evident in EU policy before it was sharpened by the COVID-19 crisis, and forms the basis of one of the priorities set out in the Commission's mandate to develop a European Health Data Space (EHDS; as described in the Commission Communication "A European strategy for data"; COM 2020a).

The EHDS should not be envisaged as a big European 'data lake', but as a system for data exchange and access which is governed by common rules, procedures and technical standards to ensure that health data can be accessed within and between Member States, with full respect for the fundamental rights of individuals in line with the General Data Protection Regulation (GDPR) and Member State competences. The objective of the EHDS is to strengthen and extend the use and re-use of health data for the purposes of research and innovation in the healthcare sector; to help healthcare authorities to take evidence-based decisions; to improve the accessibility, effectiveness and sustainability of healthcare systems; to support the work of regulatory bodies in the assessment of medical products and demonstration of their safety, efficacy and quality; and to contribute to the competitiveness of the EU's industry. It is envisaged that the EHDS will provide access to datasets necessary to make successful use of emerging responsible, human centred artificial intelligence and machine learning techniques to drive innovation in healthcare. In order to address the potential of the EHDS, the Commission is currently working with the Member States and stakeholders to define the necessary governance structures and set up an appropriate infrastructure for the EHDS.

In this context, the European Commission initiated a study to map the way in which health data governance is being addressed in the EU Member States, and how this might affect the use and re-use of health data in general and the cross-border exchange of health data in the EU in particular. The study provides an evidence-based comparison of the state of play regarding health data governance within the EU. The main purpose is to assess in what areas EU intervention might be needed and if so, through which types of measures, be it soft law such as a Code of Conduct for secondary use or hard legislative action. The focus of the study can be described by two key questions:

- What is the current state of play regarding health data legislation and governance within the EU, and what impact is that having on the way in which health data may be used and re-used for cross border health care, research or informed health policy-making?
- In what areas might EU intervention be needed and if so, through which types of measures (legislative and non-legislative action) and what governance structures or tools would that demand?

1.2. Context

The GDPR provides option for Member States for further specifications in order to adapt the application of the Regulation in (existing) national law, in particular in the area of health. At present it is unclear to what extent Member States have adopted additional regulations on the processing of health data and how this affects cross-border exchange of health data for different purposes. Accordingly, in the study we asked correspondents to identify where such legislation has been adopted and to comment on its use. They were also asked to comment on possible future actions at EU level to address the remaining challenges for data sharing, which are discussed in in chapter 8 of this report.

As several studies and commentaries have noted, the current legal and regulatory frameworks are often no longer in line with recent digital health innovations, or their introduction in the (near) future. Taking the area of telemedicine as example, different authors note that there are currently serious issues of interoperability between telemedicine solutions. The EU aims to improve interoperability and standardisation in health data exchange, and in eHealth a common eHealth EU Interoperability Framework (eEHIF) is developed. But despite such efforts to resolve legal and operational obstacles 'Member States have legal frameworks, approaches and levels of telemedicine development that are too heterogeneous to hope for effective standardisation of practices in the short term. Besides, countries sometimes adopt or adapt specific international standards according to their own needs, which represents an additional barrier to interoperability' (PWC 2018: 93).

In addition, incidents of data misuse by commercial parties, including those based outside the EU, increase the awareness that compliance with data protection rules must be ensured. The challenge for Member States and the EU as a whole is therefore to strike a balance between data security and data sharing, also as the latter is seen as a key requisite for establishing medical innovations, e.g. for vulnerable patient groups such as in specific rare diseases. While policies and regulations might be regarded as very permissive in some countries, the rules for processing health data in other countries are considered as very stringent, thus impeding the information sharing between healthcare professionals as well as for secondary purposes such as scientific research. For this purpose, some countries are reconsidering their initial adaptation of the GDPR. Finding such a balance, even at national level, is not easy nor set in stone indefinitely, but if such a balance is not met and secured in clear regulations, then this can also impose a major barrier of citizen acceptance of certain digital health innovations. Placing this into an EU context the issue is even more problematic, as divergence in legal rules governing the use of health data for secondary purposes is seen at both within and between countries. Member States and the EU are faced with several challenges in this respect. The Member States must find a balance between autonomy of citizens and the challenges of their sustainable and safe health care system. Without data sharing such systems cannot be sustained.

Solidarity in health care is expected by citizens but is not always easily compatible with autonomy.

In this light, this study examines and presents the EU Member States' rules governing the processing of health data with the objective of highlighting possible differences and identifying elements that might affect the cross-border exchange of health data in the EU, thus providing opportunity for action at EU level. As part of the study a comprehensive background assessment was conducted and complemented by an EU level discussion among relevant experts in order to map and analyse:

- Member States' national rules governing the processing of health data (for primary and secondary use) as well as specific national rules governing the rights of patients in relation to their health data (such as a patient's right to access their health data in an electronic format and share their health data with third parties).
- Strategies and governance frameworks for processing of health data. This applies to primary use as well as secondary use of health data, for example to governance frameworks of electronic health records, registries, research infrastructures and other databases in different Member States.
- Rules by which the controllers/processors of health data should abide by (such as specific rules, requirements and definitions applicable to healthcare providers).

Based on the learnings from the assessments outlined above, areas of potential future EU intervention are highlighted, including suggestions on the format of EU intervention (soft measures or hard measures), the scope (only research or broader), the actors and sectors to be included and possible policy options to realise a governance model for primary and secondary use of health data at EU level, presenting the advantages and limitations of those policy options in a comprehensive manner. This would contribute to the proper application of the GDPR, taking into account the particularities of the health sector in the Member States.

The study used a mixed-methodology consisting of literature review, case studies, surveys and workshops to provide a national mapping of legislation and governance, a discussion on best practices, bottle necks and policy priorities, and recommendations for EU level intervention. A detailed description of the methodology is provided in Chapter 2.

1.3. Scope of the study

1.3.1. GDPR as starting point

The General Data Protection Regulation (GDPR) came into effect in 2016 and became applicable across all Member States on May 25, 2018. The objectives of the GDPR are twofold: to facilitate the free movement of personal data, including cross-border exchange, and to protect the fundamental rights and freedoms of natural persons with regard to privacy and protection of personal data (Art. 1 GDPR). Member States were allowed through specification clauses to adjust the application of certain aspects of the regulation to their national situation. Furthermore, the regulation does not exclude pre-existing or newly adopted Member State law that sets out circumstances for specific processing of special categories of data in the public interest. Member States are allowed to maintain or introduce further conditions, including limitations with regard to the processing of, among others, data concerning health (Art. 9(4) GDPR).

1.3.2. Types of health data use

Throughout the report we refer to **primary** and **secondary** use of data because different legislation could apply to the different uses of health data. We explicitly distinguish between three different purposes, as outlined in Box 1.1. Function 1 is a primary use and functions 2 and 3 are secondary uses. Clear definitions are important because different laws, rules and regulations will apply dependent on the type and purpose of use. In much if not most of the literature regarding health data, primary and secondary use are distinguished. In order to be clear on other definitions, we gave an overview of the most important definitions in Box 1.2.

Box 1.1 Functions for use of health data from the health care system

GDPR Article 4(15) defines data concerning health as personal data related to the physical and mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. In practice, however, **health data** are often understood as any personal data generated within healthcare systems, and some may also include data concerning health which are collected by citizens and patients through wearable devices, apps and self-reported information. In this study a wide definition of health data is used to include all the above, as well genetic data and biometric data. The data generated in the context of healthcare includes both personal data as defined in Article 4(1) GDPR and sensitive personal data as defined in Article 9(1) GDPR. Health and social care are understood in this study in the sense of article 9(2)(h) GDPR, to include direct care provision, such as long-term care but does not include in-kind/financial benefits, such as unemployment, guaranteed minimum income etc.

Three broad functions can be distinguished involving processing of health data:

- **Function 1:** Data processing for the purposes of provision of health and social care by health and care providers to the patient concerned. This includes both in-person care and telecare using eHealth or mHealth tools.
- **Function 2**: Data processing for wider public health purposes including planning, management, administration and improvement of health and care systems; prevention or control of communicable diseases; protection against serious threats to health and ensuring high standards of quality and safety of healthcare and of medical products and medical devices.
- **Function 3**: Data processing for scientific or historical research by both public and private sector organisations (third parties, not being the original data controller), including the pharmaceutical and medical technology industries and insurance providers.

Function 1 concerns health data that are collected directly from a patient in the context of health and social care provision for the purpose of providing health or care services to that patient. This is generally referred to as a **primary use**. Such data may need to be shared across EU borders in the case of patients receiving care in a Member State other than their usual Member State of residence. This may be for planned and unplanned care of visitors, unplanned care of temporary residents, planned care in another Member State and care of patients with rare diseases as provided for in **Directive 2011/24/EU on the application of patients' rights in cross-border healthcare**, which includes also the **European Reference Networks on Rare Diseases** as well as under **Regulation (EC) No 883/2004 on the coordination of social security systems.** Such care services may be provided by public or private healthcare providers, and may be financed by public, private or hybrid entities depending on the health and care system of the Member State. Note: this includes in-person care as well as telecare using eHealth or mHealth solutions.

Functions 2 and 3 concern the re-use of health data that were collected initially in the context of providing care, but which may later be re-used for another purpose. This is generally referred to as a **secondary use**. Such secondary use may be exercised by **public entities** such as national health systems statutory payers (public bodies of health insurers), public research entities (including universities, public health laboratories), by **regulators** such as medicines agencies and notified bodies as well as by **industry.** The term **industry** includes large and small pharmaceutical and medical technology companies, companies in the insurance and financial services sector, as

well as the social media and consumer electronics actors, and the emerging AI industry. Functions 2 and 3 may use data that remain within primary use repositories, such as Electronic Health Records systems, but may also be brought together in other systems such as disease **registries** which collect data to calculate disease incidence and prevalence at **national or regional level.**
The three functions may take place when the processing falls within one of the exceptions in Article 9(2) GDPR to the general rule in Article 9(1) that health related data shall not be processed, in most cases such exceptions will apply on the basis of an EU or national law.
For clarity, note that the study is not concerned with the use of data within clinical trials when the data are collected within a clinical trial in accordance with the **Clinical Trials Regulation**; it is however interested in any legal rules and governance systems that have been adopted to allow further use of data collected for a specific clinical trial in a further trial or for another purpose.

Box 1.2 Definitions used in this study

Healthcare: for the sake of simplicity the term 'healthcare' is used to include all types of patient care, even though in some countries some of the care may be labelled social care rather than healthcare. **Healthcare provider** is defined in accordance with Directive 2011/24/EU on the application of patients' rights in cross-border healthcare to mean "any natural or legal person or any other entity legally providing healthcare on the territory of a Member State."
Healthcare professional is defined in accordance with Directive 2011/24/EU on the application of patients' rights in cross-border healthcare to mean a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife, or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment.
Data sharing is used as a generic term by which parties other than the original controller can process the data of that controller, either by performing calculations on the data by the original controller on behalf of the other party and sending the results of those calculations to the other party, or by giving the other party access to the data within the data ecosystem of the controller of by transfer of (excerpts of) the original data to the other party.

1.3.3. Legal aspects of different types of data

It should be noted that the three classifications of data use outlined above are constructs used for the purposes of analysis. The distinctions serve an analytical purpose to differentiate between functions of those data in the health care systems and to describe the respective legal bases for their use and their governance in the member states. The term 'secondary use' is not found in the GDPR, but it is to be understood as being broadly in line with the term 'further processing' of data as described in the purpose limitation principle set out in Article 5(1)(b). This states that processing data for a purpose different to that specified at the time of collection shall not be allowed when this is incompatible with the initial purpose unless such further processing is for (inter alia) research purposes and is undertaken in accordance with safeguards described in Article 89(1) GDPR. The use of health data in accordance with functions 2 and 3 will either be a form of 'further processing' or those data can be specifically collected for those functions. The legitimacy (legal bases) will generally depend on the existence of specific national legislation as provided for in Article 9(h), (i) or (j); where such legislation does not exist consent will be the default legitimation for data processing.

1.3.4. Reading guidance

Chapter 2 provides an overview of the methods used as parts of a mixed methods approach to be able to cross-validate outcomes. Chapter 3 addresses the primary use of health data (function 1); chapter 4 focuses on secondary use for public health purposes (function 2) and chapter 5 addresses the secondary use for research purposes (function 3). Next, in chapter 6 we discuss patients' rights with respects to health data in greater detail, both regarding care provision and rights surrounding secondary use. Chapter 7 deals with governance models for data sharing within and between Member States; and chapter 8 addresses the possible future actions at EU level and the support for each type of these actions among stakeholders.

2. METHODOLOGY

2.1. Introduction

A mixed methods approach was used during this study. In more detail, the following elements included:

- **Literature review** to provide an overview of best practices, bottlenecks, policy options and possible solutions already identified in the literature.
- **Mapping legal and technical aspects of health data usage at national level** to provide an overview of the differences among countries in legislation, regulation and governance models regarding processing health data.
- **In-depth case studies** of national governance models for health data sharing.
- **Workshops** held with MoH representatives, experts, stakeholder representatives and experts from national data protection offices.
- **Stakeholder Survey** to cross validate and supplement the topics addressed and identified in the Member State legal and technical aspects mapping.

2.2. Literature review

A literature review was conducted among scientific and grey literature with the aim to get an overview of what has already been identified in the literature on best practices in Member States with regard to health data use and reuse, bottlenecks, policy recommendations and solutions to identified issues related to cross-border exchange of health data. Literature has been collected through various sources. The articles were divided in 7 categories (Function 1: Primary use of health data, Function 2: Secondary use for healthcare management, Function 3: Secondary use for health research, Patient rights, Regulatory mechanisms, Practical or technical issues or challenges, GDPR analysis other that previous categories or with wider scope). Some articles fit into multiple categories.

The literature review also complements and provides references for all other components of the study, among others by acting as stepping stone towards a national level legal and governance analysis (e.g. which additional legislation is identified in the literature that needs to be addressed by country correspondents), but also by identifying issues to address during the expert and stakeholder consultations.

2.3. Mapping and legal analysis at national level

Scope of the study is the sharing of data within and between EU Member States; sharing of data with non-EU countries was not addressed. As the study commenced in December 2019, all 28 EU Member States at the time were to be covered, which at the time also included the United Kingdom. Since 1 February 2020, the United Kingdom has withdrawn from the European Union, thus becoming a "third country", to become fully effective after a transition period ending on 31 December 2020. This will impact the cross-border sharing of data with the UK, the exact nature of which is beyond the scope of this study.[2] In order that the numerical data presented in the study are not misleading going forward

[2] For the execution of clinical trials, the European Commission, EMA and HMA had recently published a technical note, referring to the implications under Directive 2001/20/EC, among others requiring that the qualified person conducting a clinical trial must be established in the EU/EEA, while the sponsor of a clinical trial or a legal representative must be established in the EU (https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-10/ brexit_technicalnotice_ct_en.pdf)

from 2020 we have placed the UK in brackets in all tables and have excluded them from all summary statistics, describing numbers of Member States; we have however included examples of data processing practice from the UK as these provide useful examples and serve to address the ranging of different data processing practices that exist both within and beyond the EU. These examples are particularly relevant as the United Kingdom had implemented the GDPR and participated in various cross border research initiatives within the EU as an EU member state at the time of the study.

For each Member State, we engaged experts with a degree in law and/or certification in the area of Data Protection or with relevant professional experience (i.e. a background in legal or compliance advisory or research or in relevant professional internal function), knowledge of the health care system, and professional competence in the national legislative language of the Member State. The experts were responsible for an analysis of the situation in their respective countries, with regard to key national legislation implementing the GDPR with respect to health data and key national governance structures that govern health data processing. To provide them guidance for this task, an extensive questionnaire was drafted, addressing the legislation concerning the three functions of further data use. The questionnaire also included a practical and technical part concerning data use and asked for opinions on several issues from the country correspondent. For each Member States, a country fiche describes the nature of health data sharing governance, based on the answers on the questionnaire (see stand-alone Annex). Correspondents of countries with a federal state structure provided information on the regulation at the federal level and the regulation in selected regions of the country. A comprehensive overview of the regulation in all regions would not have been possible within the narrow time frame. Although significant distortions are not to be expected due to this proceeding, limitations as regards comprehensiveness are unavoidable. The country correspondents closed their surveys in the first half of 2020. Changes in the legislation and the regulations that occurred after this date are not regarded. After this phase, all country correspondents were provided the opportunity to review the report and were encouraged to provide feedback and correct any misinterpretations. Last, in addition to the first survey, a second short survey (see Annex 5) was sent to the country correspondents in September 2020 with a few additional questions aiming to highlight some examples concerning the practical organisation of data sharing between organisations. The results of this survey are processed in information boxes and serve as illustration of how countries have implemented the organisation and regulation around data sharing with a special focus on data sharing from business to business and from business to government. The information was obtained from seventeen countries.

2.4. In-depth case studies of governance models

We conducted six in-depth case studies, addressing issues on governance and practical organisation of data sharing infrastructures. For the case studies we made a selection of situations, registries or authorities that can be regarded as an illustration for groups of countries in the typology. This allowed us to select specific authorities, registries and types of data to include in the case studies. We selected three Member States that have a centralised approach for data sharing and three Member States that have a decentralised approach.

For each case study, we described existing bodies (or those in preparation) with a mandate to issue decisions and/or give binding rules, recommendations and/or setting standards at national level on the primary and further use of health data, and/or

otherwise facilitate access to the health data for the primary and secondary use of health data. We did the following:

- Described the role and mission of existing bodies; identified the regulatory framework under which the office is established and operates; described the budget, sources of funding and operations (to the extent that this information is made available);

The case studies are based on publicly available data and the legal reports from the Member State experts. Supplementary information was derived from interviews with relevant authorities.

The following issues were incorporated in the reports insofar as they applied to the entity being studied:

- Mission, operations, functions and interaction with different actors (providers, research, etc.)
- Type of data used and under which conditions (approval process, anonymisation / pseudonymisation etc.)
- Strategy and specific measures to ensure the quality of health data (accuracy, completeness, relevance, validity, timeliness, and consistency);
- Data driven health economics models or strategies; type of infrastructure and the type of operations that can be performed by third parties under this infrastructure;
- Standards, interoperability frameworks and health data FAIRification strategy, as well as feedback on the success factors/obstacles (i.e. with respect to national/European legal regulations);
- Attempt to assess the cost of supervision on a comparable level (i.e. unit such as volume of authorisations per annum etc.), fees and what the fees cover, if they differ depending on actors etc. Please note, this data may be fragmented and not be comparable across other Member States.

2.5. Workshops

The aim of the workshops was to identify options for possible actions and to assess the acceptability of the proposed suggestions for solutions. Experts with diverse backgrounds participated in the workshops. These were representatives of national ministries of health dealing with health data use under the GDPR and external experts (see Table 2.1).

One full-day face-to-face meeting was organised at 29 January 2020 (workshop 1); the other two workshops were, as a result of travel and meeting restrictions due to COVID-19, organised virtually, with the third workshop spread out over 3 different occasions. The virtual meetings took place at 16 March, 29 April, 19 May and 15 June 2020.

Table 2.1 Workshop topics and participants

Workshop number	Topic(s) addressed	Audiences
1	• Discuss EU Member States' rules governing the processing of health and health-related data with the objective of highlighting differences in legal interpretation and identifying elements that might affect the cross-border exchange of health data in the EU, in order to explore areas where EU level action may be appropriate	• Representatives of Member States • Experts
2	• Explore the perspectives of stakeholders on the implementation of the GDPR and other legislation for the protection of health data, with the objective of identifying needs and differences among stakeholders and examining how these may affect cross-border exchange of health data in the EU.	• Representatives of Member States • Experts • Stakeholders from European level associations and networks
3	• Use of health data for health services (Function 2); • Use of health data for the control of communicable diseases; • Health data use for provision of care (function 1) and research (function 3); • Governance models to facilitate access for research purposes; • Exploration of further steps to be taken at EU level.	• Representatives of Member States, • Experts
4	• Current experiences on key health data processing issues and how they are addressed at national and European level; • Potential EU-level actions to improve and stimulate the (re-)use of health data.	• Representatives of Member States • Experts • Data Protection Authorities
5	• Code of conduct on the re-use of health data • Role of potential new legislation • Patient's rights • Re-use of data for research purposes • Measures needed to build an EHDS	• Representatives of Member States • Experts • Stakeholders from European level associations and networks

2.6. Stakeholder survey

In addition to the structured questionnaire completed by national level experts, a wider stakeholders' survey addressed the opinions and views of stakeholders on how data sharing is organised and on possible options to improve this. The stakeholder survey was broadly distributed among various healthcare providers, healthcare professionals, boards of disease registries, patient organisations, regulators, researchers, insurers and other relevant entities. The aim of the survey was to triangulate findings from the mapping of the legal and technical aspects and the workshops, and to identify the opinions on data use and sharing under the current GDPR and possible further actions at EU level.

The stakeholder survey, which was completed online, consisted of several separate sections. The first section was a general section, containing questions about background and geography.

This was followed by sections dedicated to different types of personal data use, and the types of EU level actions to be considered. Although not initially planned, it was decided

to broaden the scope of the stakeholder survey and cover elements on use of data with respect to COVID-19 response strategies.

2.6.1. Types of stakeholders approached

In order to identify the appropriate stakeholders for the survey, we started with a list of organisations and persons who attended the various workshops. Additional European or international level representative organisations that were found through internet searches were added to the list. The stakeholders at European or international level were asked to forward invitations to their members, or share contact details of the member organisations with our consortium. The survey was launched and circulated on 12 June to a broad audience of stakeholders in all EU/EEA countries. Stakeholders were originally invited to respond till Sunday 5 July but this deadline was extended once, till Thursday 9 July, in order to maximise responses. The survey invitations were sent by email. This invitation contained a web link to a survey made with the EUSurvey tool. The survey was also circulated via other channels, including those of DG SANTE, the European Medicines Agency and others. Social media channels were also used, and among others circulated by the @EU_Health account managed by DG SANTE, the twitter account of the European Patient's Forum and other NGOs and individuals. A copy of the survey is attached in Annex 4.

In total 543 persons responded to the online survey. The types of background are displayed below (Table 2.2). As for the geographical component, responses varied considerably, with some Member States having a higher response than others. Detailed responses per Member State are displayed in Annex 2. Given this variation, the analyses do not make a distinction in terms of the geographical backgrounds of respondents. It also implies the results cannot be considered as representative for the EU wide and thus need to be interpreted with caution. This also applies to the types of professional positions respondents may have. We were not able to validate whether the responses provided were indeed accurate, and thus if e.g. indeed 15% of the responses were provided by representatives of patient organisations or public bodies. Similarly, while 11% indicated that they were responding as individual citizens, this does not need to imply that they can be seen as lay people. In contrast, the channels used and the level of content knowledge required to answer all questions make it plausible that many of the persons answering as individual citizen are in fact professionally related to the topic, but e.g. were not able to respond on behalf of their organisations. Hence, also results in Annex 2 showing the responses per type of stakeholder need to be interpreted with caution.

Table 2.2 Response to the stakeholder survey by background (n=543)

Type	Percentage	Type	Percentage
Health professional	19%	Patient organisation	15%
Healthcare insurers	1%	Public Admin/Governmental organisation/MoH	15%
Healthcare providers	11%	Scientific researchers	20%
Industry	8%	Other/unknown	1%
Answering as individual citizen	11%		

2.7. Guidance on how to read and interpret this report

The main purpose of this study was to find out what national level legislation and governance models exist with regard to health data processing and to what extent action is needed at the European level to ensure health data protection of individuals whilst at the same time facilitating cross-border exchange of health data. This is a complex topic that involves many aspects. Therefore, as start of the study, key topic areas that needed to be included have been identified. Each topic was divided into sub-topics which define the scope of the study and make comparison between Member States possible. The following chapters will give more information on each key topic. They are structured along the lines of the legal and practical survey, which is included as Annex 3.

It is important to note that the results of this study are, to a large extent, based on individual country correspondents, who contributed as respondents to questionnaires. Taking into account the complexity of the subject, including the difficulties to find a common understanding of the terminologies involved, the authors did their best to interpret their contributions correctly and use them in the report as we did, and we take full responsibility for the interpretations. Furthermore, some responses were full of detail, others were more concise. In some instances we believe that this was related to the complexity of the situation within a Member State. As is shown in many responses, much legislation is fairly recent and in some Member States changes are underway. Moreover, lawyers in a Member State will not always agree on the exact meaning or interpretation of a law, accordingly this report reflects the considered opinion of subject matter expert lawyers, but other lawyers could take issue with some of the reported findings and argue for different interpretations.

In addition to issues of interpretation it is important to recognise that data protection in a health care setting does not exist in a vacuum. In this survey we asked correspondents to comment on the way in which the GDPR is applied in practice and to highlight where and how sectoral healthcare legislation impacts upon it. We did not ask for the full background details on all the other areas of law that affect the way in which data are used in a healthcare setting. Important other areas of law include criminal law, the law of safeguarding, as well as administrative law and tax codes. For example, criminal and safeguarding law will in many countries demand that where a case of female genital mutilation or child abuse is identified by a healthcare practitioner it is reported to the relevant authorities, regardless of the privacy interests to the patient or the parents; while laws on accounting and income declaration, as necessary in the field of health when the contribution to the health care system is income based, will demand retention of records which may be at odds with rules of data minimisation. The GDPR foresees these issues and recognises that other legal provisions will have to be balanced with the GDPR, as noted in several articles of the GDPR that allow for processing in line with national legislation. However, it was not possible to collect all the examples of interaction between GDPR and other national legislation in the context of this survey.

3. LEGAL FRAMEWORK FOR PATIENT CARE

3.1. *Introduction*

In this chapter we address data use for **Function 1** - data processing for the purposes of provision of health and social care services. We address both in-person healthcare and telecare using eHealth or mHealth tools, and look also at issues of use of genetic data, patients' rights to block access to data, and patients' rights to have data transferred from electronic health records (EHRs) to personal health records (PHRs) or similar patient accessible platforms. EHRs can be defined as a repository of digitally stored patient data (Flaumenhaft and Ben-Assuli 2018). A PHR is a similar electronic repository that is accessible directly by citizens, in some countries they are a subset of the EHR and may be seen by a healthcare professional; while in others they exist wholly independently of the EHR. EHRs contain data that are originally collected for diagnosing and treating an individual patient but can also contribute significantly to research purposes, public health purposes and monitoring of the healthcare system. This implies that the data stored in these repositories should be accessible and exchangeable among different administrative systems if appropriate conditions of the GDPR and national legislation are met. The way data are stored and coded may vary among the information systems that healthcare providers use. As a result, the availability and access and use of data vary across and within borders (OECD 2019a). Furthermore, issues concerning consent for further use and accountability play an important role. Accountability should be demonstrated (who stores what and where for what purpose) in order to assess the legitimacy of the further processing of these data (Becker 2019, Goncalves-Ferreira 2018).

3.1.1 Defining Function 1

Function 1 concerns health data that are collected directly from a patient or in some cases a patient's legal guardian where the patient is a child or is not legally competent. Such data are usually collected in a healthcare setting (such as a doctor's office or a care facility) or in an online care setting (such as a remote consultation). The data collected include both personal data, such as address and date of birth, as well sensitive personal data, which includes all health-related data. The data in question are therefore covered by both the lawfulness requirements for all personal data as set out in Article 6 GDPR and the special lawfulness requirements for sensitive data concerning health, sexual health, genetic and biometric data as set out in Article 9 GDPR.

Data collection for Function 1 purposes is generally referred to as a **primary use** of health data, since it is used for the purpose directly presented to the data subject at the time of data collection. Although the data collected at the point of care will usually be used in that setting, it may also need to be shared with other care providers for the continuity of care, with administrative services and in some cases also across EU borders when patients receive care in a Member State other than their usual Member State of residence. Such cross-border data sharing for care purposes may be for unplanned care of travellers or of temporary residents, as well as planned care where a patient travels in order to receive care. This type of care is addressed by two principle pieces of EU level legislation, **Directive 2011/24/EU on the application of patients' rights in cross-border healthcare**, which includes also the **European Reference Networks on Rare Diseases** and **Regulation (EC) No 883/2004 on the coordination of social security systems.** In addition to these two EU wide level legal instruments, a number of bi-lateral agreements exist in the EU border regions which cater to specific care across certain borders.

In such cases special data sharing arrangements may be set up to support the care of patients and may be accompanied by bi-lateral data security agreements set up between the care providers to conform with the requirements of GDPR. When data are shared for care provision, whether across borders or not, this is usually still considered a primary use of the data, since it is directly related to the data subject's care. The primary user of the data collected may be a public or private legal entity, depending on the organisation of the health system in a given Member State, similarly the care may be financed by public, private or mixed funds.

3.1.2 The legal base for data processing for Function 1

Data collection and processing for Function 1 must be legitimated on one of the legal bases of processing personal data as set out in **Article 6(1)** GDPR as well as one of the legal bases set out in **Article 9(2**) GDPR which provides an exception to the general prohibition against processing sensitive data as set out in Article 9(1).

Article 6 (1) foresees six possible legal bases for the lawful processing of personal data. All data controllers must be able to point the legal base being used for any act of data processing. Box 3.1 sets out the six legal bases of Article 6:

Box 3.1 Article 6(1) of the GDPR

Processing shall be lawful only if and to the extent that at least one of the following applies:

- 6(1)(a) The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- 6(1)((b) Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- 6(1)(c) Processing is necessary for **compliance with a legal obligation** to which the controller is subject;
- 6(1)(d) Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;
- 6(1)(e) Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority** vested in the controller;
- 6(1)(f) Processing is necessary for the purposes of the **legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. When relying on this legal basis, an assessment of the necessity and the purpose of the processing operation as well as a balancing test between the interest of the data subject against those of the controller and third parties are required.

Any one of these legal bases may be appropriate for processing personal data in a Function 1 setting, in practice several may apply to the range of data processing actions carried out under Function 1, although usually only one is named for any given act of data processing. Of the six legal bases, the one set out in Article 6(1)(d) - vital interest – will be used rarely, as it is reserved for cases of significant vital interest. Recital 46 clarifies that the vital interest's legal base applies when processing data is necessary to protect an interest which is essential for the life of the data subject or that of another natural person and where the processing cannot be based on another legal basis.

The legal bases described in paragraphs (e) and (f) recognise that some types of processing may serve important grounds of public interest or other legitimate interests of the data controller, such as monitoring epidemics or undertaking scientific research. While these legal bases may occasionally serve for a Function 1 data processing activity, they are more usually used for the sort of processing described in Functions 2 and 3 and are therefore discussed more fully in chapters 4 and 5.

Since most of the data collected for the purposes of providing care will include data concerning health, in addition to stating a legitimate basis under Article 6, a legitimate justification must also be chosen under **Article 9(2)** which provides exceptions to the general prohibition on processing special categories of data including health data set out in **Article 9(1)**. Article 9(2) provides ten exceptions to the prohibition, of which seven may be applicable to processing health data, as set out in Box 3.2.

Box 3.2 Article 9 of the GDPR - examples for processing health data for primary use

Examples for processing health data for primary use are:

- 9(2)(a) The data subject has given explicit **consent** to processing those personal data for one or more specified purposes, except when Union or Member State law provides that the data subject cannot give consent.
- 9(2)(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and **social security and social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- 9(2)(c) Processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- 9(2)(g) Processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- 9(2)(h) Processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards.
- 9(2)(i) Processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- 9(2)(j) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)** based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3.1.3 Choosing legal bases

Although the GDPR harmonises the rules governing the processing of sensitive data, such as personal health data, there are still options for Member States to lay down justifications for processing health data in Member State law. Moreover, Article 9(4) explicitly provides that with regard to processing of genetic, biometric or health data, Member States may maintain or introduce further conditions including limitations. This may mean that in the area of health the GDPR will not be applied in the same manner in each Member State. It may also mean that variations in the implementation of the GDPR may arise within one Member State, in particular where regional legislation applies. In addition, the rules under the GDPR applicable to processing of health-related data will be applied in the legal context of the provision of healthcare and the organisation of the health system in a Member State. Such health system specific legal context will set the framework for the implementation of the GDPR and may lead one Member State to lean more towards the use of consent, and another to incline more towards the legal obligation to record all aspects of interaction of a patient with the healthcare system. The national organisation of the health system may also mean that the legal base chosen varies between different categories of care providers, with publicly funded healthcare organisations applying different bases from private healthcare providers, indeed this variation was noted by the correspondent providing information on the application of the GDPR in Spain.

Given that the GDPR foresees the possibility of special legislation for processing of genetic information, it is not surprising that significant variation may exist between some Member States in this area. French and Dutch law provides further examples, since the French law prohibits the automatic processing of genetic data unless express authorisation is given by the French competent authority (Loi n° 78-17 1978[3]); and the Dutch implementing Act of the GDPR prohibits the processing of genetic data unless that processing 'takes place with respect to the data subject from whom the data concerned have been obtained'. However, both French and Dutch law contain significant exceptions permitting such data to be used for medical purposes: in France, this includes processing by doctors or biologists which is necessary for preventive medicine, diagnosis and care (Loi n° 78-17 1978), while in the Netherlands, the processing of genetic data may also take place for others than the data subject whose data it concerns if a significant medical interest prevails (Article 28, section 2 of the implementing Act (UAVG)). Medical confidentiality will then prescribe that notifying those others will be based on consent of the data subject concerned, though in exceptional cases the genetic counsellor can also fall back on the 'conflict of interests' doctrine in Dutch medical law, in essence stating confidentiality can be waived if that is the only likely way to avoid a life threatening situation of another party.

Insofar as a patient is cared for in one Member State, such variation may have limited direct impact on Function 1 data processing. However, where a patient is treated in more than one Member State, because he or she travels to access expert care, or is taken ill while abroad or avails of cross-border telemedicine care, such variation between Member States could impact patient care, as has been suggested by Bensemmane and Beaten (2019) who argue that differences in implementation of the GDPR could lead to legal issues or challenges in the setting up of telemedicine and Crico et al (2018) note similarly

[3] French Data Protection Act (Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

for mHealth. The relative newness of the GDPR means however that these comments address potential impact, the literature does not yet reveal significant cases where a difference in the implementation of the GDPR has directly hindered transfer of data, or remote access of data, for telemedicine or mHealth purposes.

This potential for fragmentation on the implementation of the GDPR has been noted in the May 2020 Communication from the Commission to the European Parliament and Council entitled "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation" which reviewed two years of implementation of the GDPR in the Member States. The report notes that the GDPR requires Member States to legislate in some areas and provides them with the possibility to further specify the GDPR in others and as a result, a degree of variation has arisen in the implementation of the GDPR which is notably due to the extensive use of facultative specification clauses.

The Commission Communication focuses particularly on variations which could create challenges to conducting cross-border business and innovation, in particular as regards new technological developments and cybersecurity solutions. While healthcare is not cited as an example, it is clear that in the context of cross-border care this variation could also add a layer of complexity, and may in turn also create issues for comparability of data in cross-border research.

Based on the variations in implementation of the GDPR that can theoretically arise both within and between Member States with respect to processing health related data in the context of Function 1, the first questions of the survey asked national correspondents to clarify which legal bases in Article 6 and 9 are used when health data are processed in the context of care provision. They were asked also to describe their national implementation legislation and give their opinion on implications for care both within their Member State and across borders, both in the case of face to face care provision and eHealth services.

3.2. Legal bases used to legitimate processing of health data for Function 1 - care provision

In this section we report on the outcomes of two surveys; one was a legal survey completed by national level expert correspondents, and one a stakeholder survey completed as an online survey sent to a wide range of stakeholders (as described in chapter 2). The findings of both surveys are complemented by a series of workshops held between February and June 2020. Both the legal and stakeholder surveys asked a range of questions on three situations in which health data are processed within Function 1:

- Data processing by a data controller who is intending to provide care to the data subject. This may be a natural person (a healthcare professional) but will more usually be a legal person (an institution such as a clinic, hospital or laboratory).
- Sharing of health data between legal or natural persons for the purposes of providing care to the data subject.
- Data processing in the context of the provision of digital health services by legal and natural persons

In addition, the legal survey also asked questions about patients' rights to block data sharing, use of genetic data and the transfer of data from a HCP held EHR to a patient controlled PHR.

3.2.1. Health data processing by the data controller who is intending to provide care

The most significant finding from the questions addressing the processing of data for in-person care provision is the wide range of answers. Results from the survey show that five Member States use only one legal base to legitimate such data processing, while fourteen use three or more (Table 3.1). The primary reason for several countries allowing for the use of more than one legal base is that the appropriate base may depend on the type of data to be used and the situation in which it is used.

The most frequently used legal bases are those related to a legal obligation to collect data in the context of healthcare provision (Article 6(1)(c)) used in conjunction with legislation on the provision of healthcare (Article 9(2)(h)). This combination was cited by country correspondents for twenty one Member States, with three giving this as the only legal base used to legitimate data processing under Function 1. The answers provided by the correspondents do not provide very granular details on the legislation related to the provision of care, but generally these pertain to legislation which regulates the interaction between a doctor and patient, which may require medical records to be kept for a certain length of time or in a certain format.

Closely related to this combination is public interest (6(1)(e)) used in conjunction with healthcare provision (9(2)(h)), which is used as the legal basis for Function 1 data processing in twelve Member States, with one giving this as the sole legal base combination. The survey did not include an option for legitimation of processing based on a contractual relationship as provided for in Article 6(1)(b), the Austrian consultant noted that it used 6(1)(b) with 9(2)(h) meaning that there is a law for processing health data for healthcare that those healthcare professionals can rely on for processing health data in context of a contract. Also the German consultant stated that the most common combination was 6(1)(b) with 9(2)(h), but added that when health data are processed in the context of employment 9(2)(b) is applied in conjunction with national law. It is presumed that other Member States may also use this combination when healthcare is undertaken in the context of employment, for example by a physician working on behalf of the employer, although other Member States did not mention this. Last, Spain noted that the legal basis of a contract was used in the context of care provided by a private care provider, which suggests that this is coupled with consent, although they did not state this is the case.

It is often contended that explicit consent is the norm for processing health-related data. This is perhaps because consent to treatment and consent to collecting data associated with treatment are conflated. The relationship between the data and treatment is reflected in the fact that correspondents for twelve Member States include consent (Art.6(1)(a) with 9(2)(a)) as one of the legal bases that may be used as the basis for collecting data from a patient and processing it for care provision, but only one (Cyprus) cited this as the sole legal base. This indicates clearly that although consent is an important aspect of data processing in the health setting, it is not dominant. The fact that consent is not a dominant legal base is grounded in the fact that consent as defined in Article 4(11) GDPR requires that it is voluntary and given in the context of a relationship where the data subject has the power to withhold consent without any detriment. Given that it is difficult to provide medical care if data are not provided, such a relationship may be hard to establish.

This was emphasised in the European Data Protection Board's (EDPB) Guidelines 05/2020 on consent under Regulation 2016/679, which emphasise that *"consent can only be an*

appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment". The inclusion of consent as one of the legal bases may therefore have to be interpreted slightly differently. It may be that consent is used as a safeguard, rather than as a legal basis for the processing of data in itself. If the processing of data is required in law, as it often is in the case of data collection in a healthcare setting, then usually consent would only be an additional safeguard (the law would be the legal basis for processing).

Table 3.1 Legal basis for normal healthcare provision

Legal basis for processing data for normal healthcare provision	Total MS	
6(1)(a) Consent and 9(2)(a) Consent	12	BE, BG, CY, DK, DE, FR, HR, MT, AT, PT, SI, FI
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	9	DK, EL, ES, HR, LV, MT, PT, RO, SI
6(1)(c) legal obligation + 9(2)(h) provision of health or social care	21	BE, BG, CZ, DK, EL, ES, FR, HR, LV, LT, LU, HU, NL, AT, PL, PT, RO, SI, SK, FI, SE
6(1)(e) public interest + 9(2)(h) provision of health or social care	12	BG, DK, EE, IE, EL, LV, LT, LU, MT, RO, FI, SE, [UK]
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	8	BE, BG, DK, IE, EL, LV, MT, RO
6(1)(f) legitimate interest + 9(2)(h) provision of health or social care	2	IE, AT
Other combination	6	DE, ES, IT, LV, HU, AT

* For information per Member State, see Table A1.1 in Annex 1

The further detail provided by the correspondents shows that all Member States have some form of national level legislation which provides a further framework for the collection and processing of data for healthcare provision purposes, which must be read in conjunction with changes that were made to data protection law made to implement the GDPR. The most striking factor emerging from the details provided is, however, that in almost all the relevant EU Member States this is well established law preceding the GDPR and much of it is also based within the constitutions of the Member States and in common law in the Member States where common law applies, with only the correspondents for Denmark and Germany reporting very recent changes to the law that regulates health data processing. This implies that the interpretation of the GDPR must be understood within the context of other laws relating to health data and the provision of healthcare that remain applicable. For some Member States the body of law relevant to health-related data processing was a single unified piece of legislation, but other Member States listed up to 30 separate pieces of law addressing specific medical areas, such as dentistry or assisted reproduction, while other had separate laws addressing public health insurers and private healthcare providers. Some of this legislation builds in an element of patient consent, which is sometimes based in the regulation of the doctor patient relationship and professional deontology as well as principles of data protection. Some Member States reported several pieces of national level legislation applicable to the processing of data for care provision purposes, in some cases based on the legal character of the healthcare provider (public or private) and in some cases on the nature of the care provided, with differentiation for more sensitive medical issues such as reproductive assistance or sexual health.

The correspondents were also asked if any national level legislation had been adopted pursuant to Article 9(4) GDPR which provides that Member States may maintain or

introduce law which contains further conditions, including limitations, with regard to the processing of data concerning health, genetic data and biometric data. A majority, sixteen of the Member States, reported that such laws had been adopted, while eleven reported that no additional laws had been put in place (see Table A1.35 in Annex 1). Where such laws have been adopted they fall into broadly three categories: laws which address the use of highly sensitive information in the context of the provision of insurance, employment or any other contractual relationship; laws which specifically address the use of genetic information in the context of assisted reproduction; and laws which require the use of special safeguards or obtaining special permission from the data protection authority when any form of highly sensitive data are used (mostly in the national laws implementing the GDPR). In some Member States the use of certain types of health-related information is prohibited entirely in specific situations. In Denmark, for example, legislation has been adopted which limits the options of employers and insurance companies to ask for or to receive specific kinds of health information (especially information which reveals information regarding potential future disorders, including genetic information). In the Netherlands such legislation existed already since 1997 and was not changed with the advent of the GDPR. As with other legislation discussed by the correspondents, some of this legislation was enacted after the GDPR, but in the majority of cases it predates the GDPR and maintains pre-GDPR rules.

Recognising that personalised medicine is growing in Europe, the survey asked if any special legislation was in place for the processing of genetic information. Correspondents indicated that twenty Member States have such legislation (see Table A1.36 in Annex 1), however, in almost all cases the legislation pre-dates the GDPR. Of those correspondents stating that their Member State had legislation addressing genetic data processing, most believed the law was adequate to allow for use of genetic data to provide personalised medicine services.

The legal survey shows therefore that the legal landscape for the processing of health-related data for care provision is complex, with many pieces of legislation applying, but also that in most cases much of this is legislation preceding GDPR. It is not surprising therefore that many Member States use more than one of the legal bases provided for in Articles 6(1) and 9(2) GDPR, and that the legal bases used depend on the legal status of the healthcare provider (public or private) and sometimes also on the nature of the medical intervention.

3.2.2. Sharing health data for the purposes of providing care to the data subject

Many patients will receive healthcare services from more than one provider and in more than one setting. The growing number of older people, ever increasing medical technical possibilities and the need for multidisciplinary approaches, and the increasing involvement of patients in managing their own care, will continue to increase the need for sharing information. The capacity to share data among care providers and patients is seen by many as an important aspect of improving patients' safety, reducing the number of avoidable mistakes, and improve the coordination and continuity of care (OECD 2017). In order to establish if the implementation of the GDPR had impacted such data sharing, the survey asked correspondents to describe the legal base under Articles 6 and 9 GDPR used to legitimate the sharing of data between healthcare providers.

In this context we saw a slight reduction in the range of bases used, with eleven correspondents reporting that just one legal base was used, and eleven reporting the use of three or more different legal base combinations. There was also a slight up-tick in the use of consent as one of the legal bases, with seventeen reporting the use of consent

when data are shared. The most commonly cited combination of legal bases was again legal obligation plus healthcare ((6(1)(c) plus 9(2)(h)) as with the processing of data for direct care provision, with five using this as their sole legal base.

The respondents were asked to describe the national level legislation regulating such data sharing. The descriptions make clear that the relatively high level of reliance on consent needs to be understood broadly, not simply as consent to share data within the framework of GDPR. Most correspondents citing the use of consent noted that this was consent within the context of care referral, so not necessarily consent solely to share information, but closely linked to consent to be referred to another care provider. The law of Belgium, for example links the two consents, requiring that a patient must agree to the participation of a new care provider in his or her treatment or information about such treatment (Article 10 of the Law of 22 August 2002 on patient rights). An interesting note was provided also by Netherlands, where the correspondent stated that health data may be shared within a care team working under one data controller (i.e. the care team with whom the patient has a contract), however, if such data are shared with another care team working for a different care provider, the patient's consent must be sought. However, that consent may be presumed if the patient has agreed with the referral. This applies to push systems. The data are sent to a new known health care provider to which the patient has been referred. If on the other hand the data are made available to be accessed by a possible new health care provider, generally described as a pull system, the consent of the patient is necessary. For Italy it was noted that all health records are configured, ab initio, as a PHR; accordingly, the patient has control over all access to the record and refusal of consent to access to the record means that the treating physician cannot access previous records contained in the PHR. Yet, the assisted person is entitled to receive care even in absence of such consent for the access to the PHR.

The legislation on health data sharing described by the correspondents in many cases also described situations in which data are used for purposes beyond patient care, and therefore has a significant overlap with Function 2 type of data sharing – that is sharing for the purposes of health care system management and public health. Much of the legislation also referred to the governance of EHRs and the fact that authorised health care providers have access to EHRs, which means that records are not shared as such, but accessed by different authorised care providers. In the Netherlands, for example, we saw the distinction between sending patient data (push) and retrieval of patient data (pull). There is a national Node (Landelijk Schakelpunt) which does not contain health data of patients but via which such data can be retrieved. The patient's consent is needed to retrieve data via this system or via regional systems which exist as well. The original Act which concerns these systems states that the consent can be granular meaning that the patient should explicitly consent which health data can be retrieved by which health care providers. That provision of the Act will never enter into force. It was found to be completely impractical also for the patient with over 170 options to choose from. The Act on safe data exchange is under further consideration at the moment, such as whether this consent principle should also apply to emergency situations. There had already been a temporarily exemption to this principle in the case of emergency COVID-19 treatment. A similar situation occurs in the majority of other Member States, as seen in Table 3.2 below which shows that 13 of the 17 Member States marked as using consent also use another legal base. A further interesting issue is the overlap with public health law, which is evident in some countries who regulate health data sharing by disease category or patient category.

Table 3.2 Legal basis to share health data between healthcare providers or professionals.

Legal basis for processing health data between healthcare providers	Total MS	
6(1)(a) Consent and 9(2)(a) Consent	17	BE, BG, DK, DE, CY, FR, HR, IT, LV, LT, MT, NL, AT, RO, SI, FI, SE, [UK]
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	7	DK, EL, HR, LV, PT, RO, SI
6(1)(c) legal obligation + 9(2)(h) provision of health or social care	19	BE, CZ, DK, IE, EL, ES, FR, HR, LV, LT, LU, HU, AT, PL, RO, SI, SK, FI, SE, [UK]
6(1)(e) public interest + 9(2)(h) provision of health or social care	8	BG, DK, EE, IE, EL, LV, RO, SE,
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	7	BE, BG, DK, IE, EL, LV, RO
6(1)(f) legitimate interest + 9(2)(h) provision of health or social car	3	IE, LV, AT
Other combination - please specify	4	DE, ES, LV, AT

Patients' right to block data sharing in the context of their care

The importance of the legal base of consent for data sharing for care provision purposes was further clarified in an open question which asked if any legislation exists that allows a data subject to block such data sharing. Of the 22 correspondents who replied to this question, five indicated that it is not possible for a patient to block such data sharing. The majority of the 17 respondents who replied positively indicated that this was a balanced right. Several countries mentioned that in a normal setting sharing of data with another health professional is based in a culture of consent (rather than a strict legal requirement to obtain consent), that is a patient is informed about the intent to share data when a patient is transferred to another healthcare provider, but few indicated that this was an absolute duty which can never be overridden. Several Member States, including Romania and Hungary indicate that data sharing with another healthcare professional is usually based on consent, but that the legislation provides for situations where consent is not required, for example for certain diseases. The Swedish response is interesting in that it states that data may be blocked, but that fact that block data exists must be visible to other healthcare providers. Some correspondents noted that data blocking by the patient can only happen where the data are not needed for the continuity of care of the patient. This among others applies to CZ where patients cannot block reports of health services received from a care provider other than their general practitioner being reported to their general practitioner. The correspondent for ES stated that the right does not exist per *se*, but noted that a right to refuse treatment exists and when such right has been exercised data sharing is effectively blocked. Some also noted the extent and nature of the blocking may be related to the data concerned; the correspondent for IT noted for example that HIV data or sexual violence data may be obscured by the patient when sharing data.

In some cases administrative law will oblige a healthcare professional to share data, such as in Slovakia, where Act No. 576/2004 on Health Care requires that in the case of general practitioner (GP) change, the previous GP has the legal obligation to hand over the written medical records or its copy to the new GP within 7 days following the request; a later law act No. 153/2013 on National Health Information System extends this rule to electronic medical records.

Transferring health data from the Electronic Health Record (EHR) into a "personal health environment (PHE)" or other form of citizen-controlled record

Within the context of sharing data, country correspondents were also asked to comment on transferring health care provider controlled data held in an EHR to a record controlled by patient, such as a PHR or other system by which a patient can directly access data held by HCPs (Table 3.3). Eleven correspondents reported that this was possible, or will be possible when legislation that is currently in the adoption process enters into force, while fifteen reported it was not possible to do so, with one Member State (NL) noting that PHR-like systems exist and are supported by public funds and policy, but are not directly enshrined in law.[4] Others stated that while there was no export mechanism to a PHR, the patient has a secure access to the health care provider held EHR (RO and SL). Germany reported quite extensively on new legislation that has been adopted and is now being further spelled out, and that includes capacity in future years for a patient to be able to label certain data as accessible to researchers; this issue is discussed further in chapters 5 and 7 below.

Table 3.3 Legislation or rules that facilitate data from the Electronic Health Record (EHR) to be exported into a "personal health environment (PHE)" or another form of citizen/patient-controlled record

Legislation / regulation for sharing EHR data with a PHE	Total MS	
Yes, regulation/legislation is in place that facilitates export of EHR data to a personal data health environment	8	BE, DE, EE, FR, HR, IT, AT, SI
Not yet – but legislation is currently being developed that will facilitate the export of EHR data to a personal environment	3	CZ, CY, NL
No – there is no formal regulation/legislation for export of EHR data to a personal health environment	15	BG, IE, EL, ES, LV, LT, LU, HU, MT, PL, PT, RO, SK, FI, SE, [UK]
Not sure	1	DK

Cross-border data sharing between health providers or professionals

The discussion above shows that the full range of potential legal base combinations across Article 6(1) and 9(2) GDPR is used by the Member States for sharing data for the purposes of providing care to the data subject. This naturally leads to questions of how cross-border data sharing for planned or unplanned care is handled. While in practice the numbers of patients accessing cross-border care remain very low[5] the country correspondents nevertheless felt that the GDPR can cause issues when cross-border transfer of patient data is necessary. Fifteen Member States commented that the range of potential legal bases in GDPR and the different application of those bases between the Member States could hamper the flow of patient data for care or research purposes between Member States, and thirteen believing it could hamper data flow within their Member State too with some expressing this more forcefully than others.

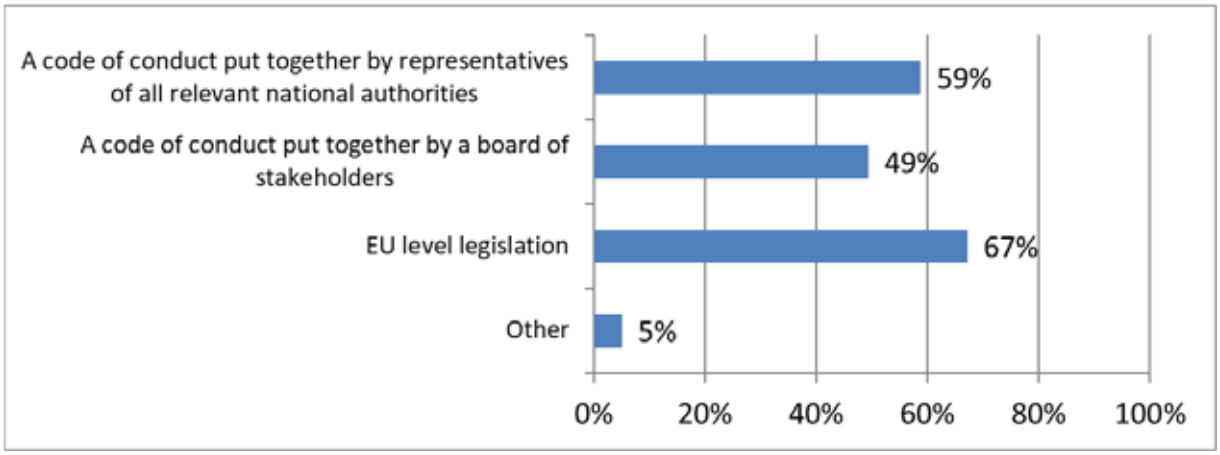
[4] The relevant initiative in the Netherlands is https://www.medmij.nl/en/, in which all citizens must have direct online access to their GP electronic health records and a set of technical rules and regulations has been established (medMij). It is based on so called ' field norms' and not yet on legislation and PHE providers can be accredited. The UK correspondents adds that the NHS England has committed to all patients accessing their own care plan and communications from care professionals via the NHS app by 2020/21, and by 2023/24 patients will have access to digital-first primary care (according to the NHS Long Term Plan published in January 2019).

[5] See https://ec.europa.eu/health/sites/health/files/cross_border_care/docs/2018_msdata_en.pdf

The sentiment is similar among the stakeholders responding to the online survey were to rate the ease of sharing health data for care provision purposes with another EU Member State on this question half rated the ease of sharing as above 6 on a scale where 1 = easy and 10 = impossible. The stakeholders were also asked to comment on this issue, and amongst that group 77% agreed with the statement that '*the use of different legal bases (e.g. consent, provision of care, public interest) make it difficult for health-related data to be shared for care purposes between EU countries'.*

Broadly speaking, the experts consulted - whether national level consultants or stakeholders in the online survey and workshops - often showed some level of dissatisfaction with the current legal and organisational frameworks which govern health-related data processing at national and EU level. When asked if the exchange of patient data for care or research purposes is made difficult because of the use of different legal bases between different data controllers within their Member State, twelve correspondents reported that they believed this to be the case, while seventeen thought that the current legislation in place in their Member State and at EU level was not sufficient to facilitate a free flow of health-related data between Member States. The correspondents showed a keen interest in further action at EU level to address these shortcomings, with ten indicating that they thought an EU level code of conduct could be helpful and thirteen thinking new EU level legislation to address better flow of health data between Member States would be useful. Stakeholders also favoured legislation, with 67% of survey respondents indicating that EU level legislation would be an appropriate governance tool for an EU level data sharing infrastructure and governance (see Figure 3.1).

Figure 3.1 Share of stakeholders agreeing with the following statements, all related to how the governance of an EU level data sharing infrastructure should be assured if it was set up



3.3. Data processing in the context of the use of digital health solutions

Digital health solutions are becoming a key element of health services across the EU, with many Member States using remote monitoring and mHealth to support patients with chronic conditions, notably in the use of implantable and wearable connected devices such as pace makers and continuous blood glucose monitoring devices, as well as less invasive support tools including connected weighing scales or apps for patient reporting of symptoms. Here again a surge of activity has been seen with the advent of the COVID-19 pandemic which has increased the use of symptom reporting apps, as well as connected devices to support chronic care patients.

To examine the impact of GDPR on the operation of digital health services correspondents were asked to state if any specific legislation had been adopted to address the processing of health data in the context of a digital health service. Twelve correspondents[6] reported that specific legislation to accommodate data processing in digital health services had been adopted, while fourteen reported[7] none had been adopted. However, it was noted that it is not always easy to give a clear answer, with one correspondent commenting that the legal regulation of the use of apps and devices may take very different forms, noting that in some situations, the GP may mention or recommend that the patient install an app or buy a device to monitor e.g. exercise performance, while in other situations a hospital may prescribe the use of an app to monitor glucose levels, and the information is automatically transferred to the patient's EHR. The legal basis in the GDPR for the processing of these data will differ depending on the situation. A follow-up question noted that a healthcare professional may in some cases prescribe the use of an app or a device which collects patient data. The patient's consent to the use of such an app or device will be based on national level medical law, however, the processing of the data from such apps or devices must also be legitimated under the GDPR. The survey therefore also asked which legal bases in Articles 6 and 9 GDPR were used to legitimate the collection and processing of health-related data via apps or medical devices. In spite of the other options offered by the GDPR, consent was by far the most common legal base, with eighteen citing Articles 6(1)(a) plus 9(2)(a), of whom thirteen gave this as the sole legal base combination used.

Table 3.4 Legal basis used for processing app or device derived data in the healthcare setting

Legal basis for processing app or device derived health data	Total MS	
6(1)(a) Consent and 9(2)(a) Consent	18	BE, CZ, DK, DE, CY, EL, FR, HR, HU, MT, NL, AT, PL, PT, RO, SI, FI, SE
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	3	BE, DK, IE
6(1)(c) legal obligation + 9(2)(h) health or social care	6	BE, DK, IE, ES, SK, FI
6(1)(e) public interest + 9(2)(h) health or social care	5	DK, EE, IE, IT, FI, [UK]
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	1	DK
6(1)(f) legitimate interest + 9(2)(h) health or social care	2	DK, IE
Other combination	2	DE, LU

While the collection of data via an app or implanted device is often based on consent, the literature shows that it is not always easy for a patient to exercise all their rights with respect to data collected via an implanted device, in particular the rights of access and data portability. In many cases the data collected by a device, such as an implanted cardiac device, is sent by the device to a data platform controlled by the device-maker from which the processed data will then be sent to the healthcare professional. While patients may access the reports about such data that are recorded in their healthcare records through the normal channels for access to healthcare records, access to the full

[6] CZ, DE, EE, EL, FR, HR, LT, AT, PL, RO, SI, SK

[7] BE, BG, DK, IE, ES, IT, CY, LV, LU, HY, MT, NL, FI, SE [, UK]

data sets is often difficult, and portability of the data for use on a different care platform can be very difficult to ensure.

To explore this issue correspondents were asked if patient access to the data held on the device maker's platform can be assured. While ten MS correspondents were not clear about how this was handled, eight reported that such access was always assured and eight commented that it was not always possible to facilitate such access to data for a patient via the health care provider (Table A1.37 in Annex 1). Hence the patient should rely on the general clauses of the GDPR. This is certainly an issue which must be explored further. The patient might not be aware that the data which the health care provider receives and to which he or she has access, are often first mediated by the platform of the device maker. And if the data would be pseudonymised, Article 11 of the GDPR might apply for data arriving at the device maker's platform, which would make access and portability of such raw data illusory. As was discussed during the third workshop there is also discussion about the legal status in the GDPR sense of the device maker at that intermediary stage where the raw data of the device are transferred into intelligible data for the health care provider and patient. Does the device maker act here as a controller of the data or as a processor? The correspondent for Germany mentioned a recently adopted regulation addressing digital health as follows:

> *"The procedure for the inclusion of a digital health application in the directory for digital health applications of the Federal Institute for Drugs and Medical Devices is initiated upon application by the manufacturer. Relying on § 5 I and § 6 of the Digital Health Application Ordinance, the manufacturer shall state in the application whether data processed via the digital health application can be exported by the insured person from the digital health application in an interoperable format and made available to the insured person for further use by 1 January 2021 at the latest. They shall also state whether the insured person can export relevant extracts of the health data processed via the digital health application for their care, in particular data on therapy courses, therapy planning, therapy results and data evaluations carried out, from the digital health application from 1 January 2021 at the latest."*

Germany is however unusual in having such detailed legislation, as other countries, such as Austria rely on guidance documents which are addressed to the device makers and define, among other things, interoperability standards and processes for transmitting data (measurements) from devices (e.g. of pace makers), rather than explicit legal requirements. England similarly addressed this issue through the device and apps requirements that must be met before they can be given to a patient within the context of NHS healthcare provision. In order to be accredited as an NHS compliant app the app developer/provider must submit the app for assessment by a third party accreditation body. The assessment criteria include being able to ensure patient access to data generated by or held on the app. This certification mechanism does not however apply to an implanted device which, as a medical device, will be assessed by a notified body under medical devices legislation rather than through an app assessment procedure.

On a wider level the correspondents were asked if they were aware of issues relating to GDPR having an impact on the provision of digital health services generally, not related to apps and devices. Sixteen stated they were aware of issues, of whom twelve thought the GDPR impacted at both national and cross-border on the use of digital health tools. The Czech correspondent noted that much of the impact was due to a lack of understanding on how the obligations to meet GDPR requirements are met by both a digital health tool provider and a heath care professional. In particular the correspondent noted that a healthcare professional with data controller liabilities may be reluctant to accept responsibility for data safety and security when data are processed on a device

maker's platform, similarly for the accuracy of data. Sweden and Slovakia both mentioned the fact that digital health service providers often process data outside their Member State and that this often leaves healthcare providers confused about how to ensure they meet the requirements of the GDPR when they retain the role of data controller and the device provider is acting as data processor. While the GDPR may set out the rules for territorial scope quite clearly, and the EDPB has issued guidelines[8], a healthcare provider may often feel they are exposing themselves to levels of risk beyond their comfort. Similarly, with respect to the speed to development of technologies in digital health, the correspondent from Italy pointed to an imbalance between GDPR requirements of data minimisation and purpose limitation, and the way in which Artificial Intelligence (AI) based digital health systems are developed which depend on maximum data availability.

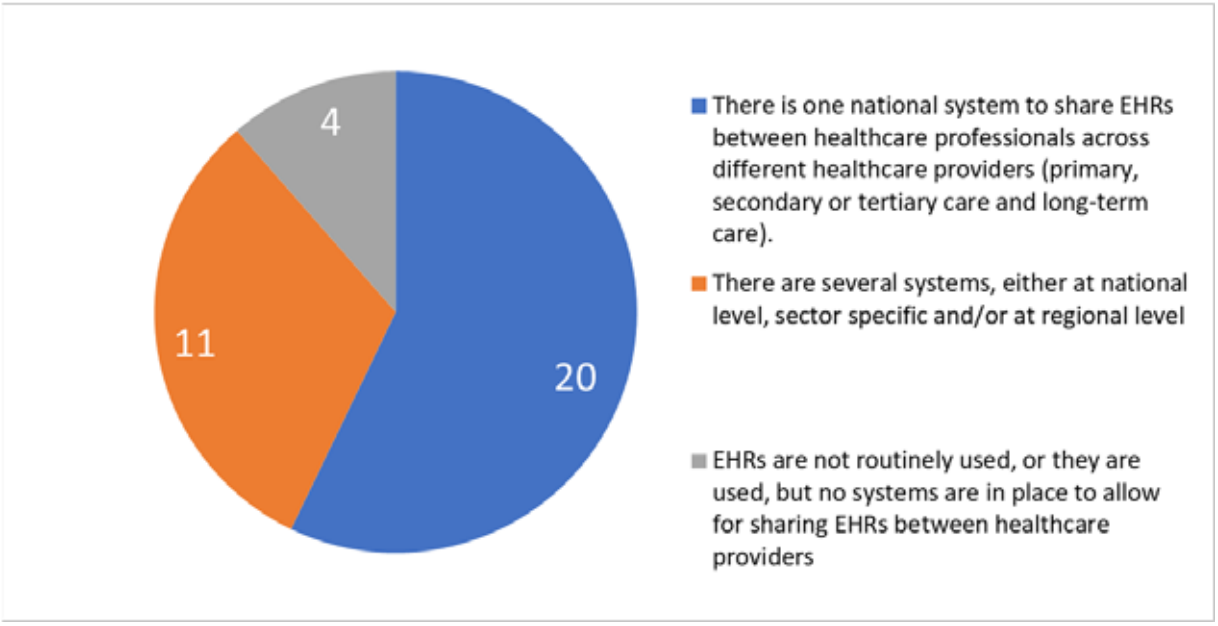
3.4. Practical and organisational aspects of data use for care provision

In this section we present results from the questionnaires and workshops regarding the sharing of health records for function 1 in a more practical sense. We focus on three important aspects of data FAIRness: Findability, and Accessibility and Interoperability, all three of which affect the Reproducibility, which is the fourth element. Also, we focus on the use of EHR data for function 1. It should be noted that data FAIRness is not only relevant for function 1, but also for functions 2 and 3.

As noted in the introduction to this chapter, Electronic Health Records (EHRs) are a core building block for disease monitoring, surveillance, health and health services research, as well as for the provision of care for individual patients (Blumenthal 2017, Verheij et al 2018). In almost all Member States there are ICT systems by which healthcare professionals can share the electronic Health Records (EHRs) of individual patients with other healthcare professionals. This may be done with one national system or use several national, regional or sectoral systems. Figure 3.2 shows that the majority of 27 Member States report having a system in place through which EHR data can be accessed and shared between health care professionals: 20 MS have a national system across different sectors, while 11 MS have several systems place, either at national level, sector specific and/or regional (which can exist in parallel with a single national system). In 4 MS EHR data are not routinely used, or if they are used, there is no system in place to allow for sharing EHRs between health care providers (see Table A1.26 in Annex 1 for detailed responses).

[8] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1 12 November 2019

Figure 3.2 ICT systems by which healthcare professionals can share EHR data of individual patients with other healthcare professionals



3.5. Interoperability, security and data quality in the context of care provision

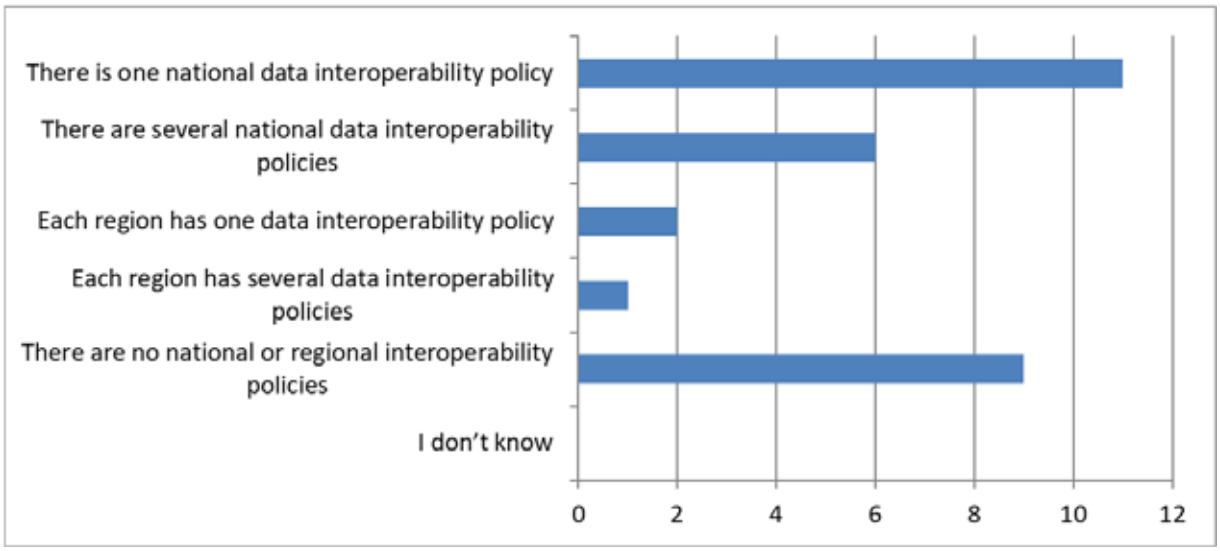
In order to build confidence in the use of EHRs, it is of paramount importance to ensure that the interoperability of EHRs can be assured and data quality guaranteed. They are among the cornerstones of the use and reuse of health data for all three types of use, function 1 discussed in this chapter, as well as functions 2 and 3 discussed in chapters 4 and 5.

A number of general and sectoral Standards Development Organisations have developed technical standards, norms and guidelines to drive interoperability, security and quality of health records and other health data exchange infrastructures. It among others refers to CEN/ISO (health informatics standards), HL7 (health information exchange standards), CDICS (health data research standards) and OpenEHR (electronic health records standards). Yet, a lack of widespread data standards adoption still forms a barrier to data sharing among countries and within countries, especially when the healthcare system is fragmented (Genevieve et al 2019). Alongside interoperability, security and quality are identified in the literature as further important features for health data sharing. Trust in security, and especially on the protection of personal data, is important for individuals in their decision to share their data for further data use (Forcier 2019). Closely related to security is the concept of accountability (Cool 2019, Hoeyer et al 2019), it should be clear who is accountable for what and how one can trace this.

To address the demands of interoperability, security and quality many countries have adopted policies, guidelines or legal requirements that ensure standards and that are used by healthcare provider organisations. In our mapping we provided insights in the adoption of such policies to ensure the use of technical standards to support interoperability of health data, as well as security and quality. In about half the Member States, there are national or regional interoperability policies regarding the technical standards to be used to ensure that the structure and format of data are interoperable so that such data may be shared between healthcare professionals or incorporated into more than one database for secondary use (see Figure 3.3). About one third of Member States has no national or regional policies to ensure interoperability. In most Member

States such policies exist, and in many of them there is some sort of national policy, often in combination with a regional or sectoral policy.

*Figure 3.3 National and regional interoperability policies which address use of standards and interoperability across all healthcare provider sectors (primary, secondary, tertiary, and long term care)**



* For information per Member State, see Table A1.28 in Annex 1

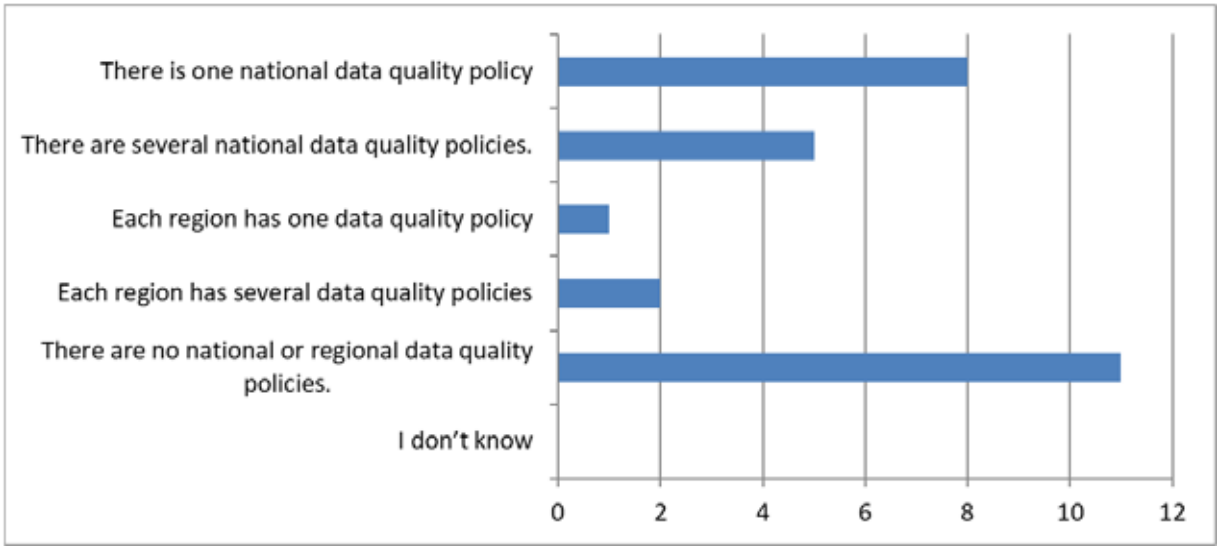
The majority of Member States have a national health data security policy, regarding technical standards to be used to ensure health data for primary use are processed and stored securely (see Figure 3.4). Initiatives vary from stimulating stakeholders to promote interoperability (as in the Netherlands) to legislative obligations (as in Germany).

Figure 3.4 National or regional health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely across all healthcare provider sectors (primary, secondary, tertiary, and long term care) (not sure treated as 'missing')

* For information per Member State, see Table A1.29 in Annex 1

In Member States there may be one or more national data quality policies regarding the technical standards to be used to ensure the quality of health data for use in EHRs or other digital applications. National data quality policies exist in a minority of countries. A considerable number, however, have only regional or sectoral policies in place (see Figure 3.5).

Figure 3.5 National or regional data quality policies regarding the technical standards to be used to ensure the quality of health data for use in EHRs or other digital applications across all healthcare provider sectors (primary, secondary, tertiary, and long term care) (not sure treated as 'missing')



* For information per Member State, see Table A1.30 in Annex 1

3.6. Concluding remarks

In this chapter we focused on function 1, the use of data for patient care and discussed the legal bases for this type of use. While many countries include informed consent amongst the legal bases for this type of use, all but Cyprus report that they also include another legal base to legitimate data collection for the purposes of healthcare provision in specific sectoral legislation as provided for in Articles 9(2)(h) and (i) GDPR.

This extends also to the sharing of data between healthcare providers for care provision, although in this case four Member States (CY, IT, MT and NL) state that consent is the sole legal base for such data sharing. As we move towards health data that is more directly controlled by the patient, such as data from apps and devices, or data shared between EHRs and PHRs, we see a greater reliance on patient consent and less frequent use of specific sectoral legislation, this may however be an artefact of the relative newness of such data within healthcare provision, compared to the traditional physician held medical record which is many centuries old. What is most significant from the reports on the governance of data used for care, is the variety of legal bases used. The reasons for this would seem to be two-fold; first, healthcare services are operated in a complex regulatory setting with many laws and guidelines dictating how services are provided, and the way in which data are handled has to fit into that system. The drafters of the GDPR were mindful of this back catalogue of legislation applicable to the healthcare setting and accordingly provided for the adoption of EU or Member State level legislation to justify the processing of health related data for care provision, public health and scientific research purposes. The result is however, that sharing of health related data for care purposes across EU borders may be hindered by a lack of compatibility between legal bases chosen and the detail of national laws. As shown above, this is a

matter of some concern for stakeholders, of whom 77% agree that lack of compatibility in legal bases make it difficult for health data to be shared across EU borders for care purposes.

In addition to the legal fragmentation identified in the reports, the country correspondents also noted a high level of complexity in the practical aspects of the exchange of information between health care providers and between health care providers and patients. Many countries have more than one healthcare record, often creating issues of data flow within a Member State as well as between countries. In the cross-country setting this will often lead to lack of technical interoperability between record systems, as well as operational interoperability for allied issues such as patient identification and health care professional authentication. A very likely consequence is that the exchange of information about individual patients between health care professionals working in different settings is a challenge which may significantly impede the potential for patients to exercise their rights to cross border care as set out in Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, which includes also the European Reference Networks on Rare Diseases as well as under Regulation (EC) No 883/2004 on the coordination of social security systems

The GDPR itself, as well as sector specific legislation on cross border care and the EU Treaty itself provide opportunities to overcome these issues of fragmentation. As noted in Articles 9(2)(g)-(j) GDPR the provision is made for Union or Member State law to further address the processing of health related data in certain situations. Furthermore, the GDPR also provides for the creation of Codes of Conduct by relevant stakeholders to address particular needs of data processing, which may be granted EU level validity through implementing legislation as provided for in Article 40 (9) in accordance with Regulation 182/2011 which lays down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers. The input of the country correspondents, stakeholders as well as the comments made by participants in the workshops clearly showed that there is appetite for the European Commission to explore the potential of new legislative acts to address the issues raised.

We recall that correspondents for eighteen Member States reported that the current legislation in place in their Member State and at EU level was not sufficient to facilitate a free flow of health-related data between Member States, and 67% of the stakeholder respondents indicated that EU level legislation would be an appropriate governance tool for an EU level data sharing infrastructure. The survey did not specify the purpose of data sharing infrastructure, accordingly the interest can be interpreted as being for all three functions.

4. FRAMEWORK FOR SECONDARY USE OF HEALTH DATA FOR PUBLIC HEALTH PURPOSES

4.1. Introduction

It is widely acknowledged that safe, efficient and sustainable healthcare systems are highly dependent on data (Delvaux et al 2019, OECD 2019a). Data may support clinical decision making, may allow for healthcare system planning, supervision and improvement and may provide information to empower patients to engage actively in their healthcare and wellness management.

As described in the introduction, **function 2** is the processing of data for wider public health purposes including planning, management, administration and improvement of health and care systems; prevention or control of communicable diseases; protection against serious threats to health and ensuring high standards of quality and safety of healthcare and of medical products and medical devices. This concerns the re-use of health data that were collected initially in the context of providing care, but which can later be re-used for **secondary use** exercised by **public entities** such as national health systems statutory payers (public bodies of health insurers), public health bodies (including universities, public health laboratories) and by **regulators** such as medicines agencies. The use of data in Function 2 includes both data that are collected specifically for function 2 purposes, and the re-use of data collected for the purpose of providing care (function 1) for another purpose. For example, use of EHR data for tracking vaccine uptake could be re-use of data collected for care purposes, where as a dedicated vaccination database used for public health tracking purposes would be a primary use of data.

Article 9(1) of the GDPR notes that in general processing of data concerning health or genetic data shall be prohibited, but provides in **9(2)** that this prohibition will not apply if the data subject has given explicit consent or, in the case of health related data, that additional EU or national level legislation has been adopted that addresses the processing of health data for the purposes **of providing healthcare (9(2)(h)) or for public health reasons (9(2)(i))** (see Box 3.2 for a more detailed description Article 9). This report distinguishes the following types of such secondary use:

- Management, administration, reimbursement;
- Improvement of the health and care systems;
- Market approval of medical device and medicines;
- Medical device monitoring and pharmacovigilance (PMS);
- Protection against serious cross-border threats to health;
- Disease registries.

4.2. Management of the health care system

Health system management and health care cost reimbursement should be distinguished from wide reaching initiatives to drive improvement of the health care system. The latter may involve value judgements (what is seen as an improvement by some might not be seen as an improvement by others) while the former is just needed to make the health care system function. Using data for planning of the health care system is yet a different purpose that is part of the broader management of the health care system. The data involved for any of the three purposes can either have been recorded already for function 1, but they can also be especially collected for function 2.

Table 4.1 Legal basis for processing data that was originally collected for the purpose of providing care (function 1) to allow it to be used for planning, management, administration and improvement of the health and care systems.

Legal basis for healthcare management	Total MS	
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	16	CZ, DK, DE, IE, EL, ES, HR, LV, LT, LU, HU, NL, PL, PT, SI, SK, FI
6(1)(c) legal obligation + 9(2)(h) healthcare	9	DK, IE, EL, ES, FR, HR, LV, LT, SI, SE
6(1)(e) public interest + 9(2)(h) healthcare	13	BG, DK, EE, IE, EL, ES, FR, HR, LV, LT, MT, AT, SE, [UK]
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	12	BG, CZ, DK, EE, IE, ES, LV, LU, MT, NL, AT, FI, [UK]
6(1)(f) legitimate interest + 9(2)(h) healthcare	1	IE
Other combination*	6	DK, DE, EL, ES, IT, MT
No specific legislation	3	BE, CY, RO

The question addressed by the country correspondents had a broad scope, which is reflected in the diverse range of answers received, with many respondents mentioning more than one legal basis (see Table 4.1). The legal bases used within one Member State will depend upon the type of processing: for management and planning of the health care system, reimbursement or improvement.

The legal bases used will also depend upon the actors involved and characteristics of the health care system. There will be differences between taxation based and insurance based systems and whether there is a large private health insurance sector. In the latter case legitimate interest (6(1)(f) GDPR) will often be the residual legal basis combined with an additional justification under Article 9(2) GDPR for the processing of health data.

Except for three Member States (Belgium, Cyprus and Romania), all responded that there is legislation concerning planning and reimbursement, which is unsurprising in the light of the Court of Justice of the EU ruling in *Smits and Peerboom* that hospital care needs to be planned in order to allocate resources adequately and to prevent, as far as possible, any wastage of financial, technical and human resources.[9] It is difficult to imagine a system which does not use real world data on health care use for such planning. Such use must meet the criteria of necessity and proportionality and must employ privacy by design and by default (article 25 GDPR, Guidelines EDPB on privacy by design and by default, 2020). Yet it cannot be assumed that the data will always be anonymised, not least because planning requires that double counting is avoided. It is necessary to distinguish one patient visiting three hospitals for the same health problem, from three different patients visiting three hospitals for the same health problem. This makes using truly anonymous data unlikely (see chapter 8 on the discussion about anonymous and pseudonymised data).

In the absence of any specific legislation, implementing 9(2)(h) or 9(2)(i) GDPR, only 9(2)(a)GDPR, explicit consent, would be the basis to share health data to meet the needs of planning and reimbursement. Furthermore, in the case of reimbursement the validity of consent would be questionable as valid consent means that the data subject should also be able to refuse to give consent without negative consequences (European Data Protection Board's (EDPB) Guidelines 05/2020 on consent under Regulation 2016/679). Obviously there are negative consequences as not providing consent to data being submitted to the reimbursement authorities means that one has to pay health care expenses oneself. Some respondents also considered 'disease registries' under this question. That might be the reason that also informed consent was mentioned as an

[9] Case C-157/99. See also answer provided by the Commission to a parliamentray question at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:084E:0953:0954:EN:PDF

additional legal basis in the additional comments to the table. We will come back to disease registries in section 4.4.

The statutory basis of data processing for planning and reimbursement is reflected in Table 4.1 which shows that the patient usually cannot object to such use when the processing is based on a legal obligation laid down in national law. From the comments and more detailed answers of the country correspondents, we learned that opt-out would usually apply for specific applications of data use or improvement of the health care system. Our searches found no literature which specifically addresses data processing for the planning of the health care systems and reimbursement. It therefore may be concluded that it is taken for granted that in European health care systems, which are based on solidarity and universal access, must contain the costs of system and prevent fraud. For performing these tasks, schemes for data exchange with planning and funding/reimbursement bodies must run in the background of other data uses, requiring the re-use of health-related data in line with national legislation and the GDPR.

Issues arise however with further use of those data to further improve the system and make the health care systems sustainable in the long run. That purpose requires more intensive further use and the combining data from various sources. As will be shown in the later sections of this chapter, there are many hindrances in that respect.

4.2.1. Health data sharing with public bodies

Health system management often includes collaboration between healthcare provider and public health bodies. In order to explore the legal framework for these interactions, the country correspondents were invited to respond to an additional question to expand on the response shown in Table 4.1. Box 4.1 below gives a snapshot of responses, which illustrates the complexity and range of legal relationships that are maintained in the context of a publicly funded health system.

Box 4.1 Examples of specific legislation that obliges healthcare providers to provide patient data to public health authorities*

Twelve countries provided additional information on whether there is sectoral legislation that obliges a health care provider to give public health authorities access to patient data for the management of the health care system. In ten of the responding countries this type of legislation exists (Bulgaria, Ireland, Italy, Greece, Hungary, Lithuania, the Netherlands, Poland, Slovakia, and Sweden). In **Bulgaria** this can be related to the use of data for the needs of public healthcare (under the National Health Act, art. 28/4). The information must be anonymised or de-identified. This is similar to the situation in Ireland. In contrast, in Lithuania, the State Accreditation Service for Health Care Activities has the right to receive all information, including personal data from healthcare institutions when this is required to assess compliance with the requirements of the legislation (under the Law on Health Care Institutions in order to ensure the adequacy of personal healthcare services and patient safety). In **Italy** also a comparable situation exists for data within the FSE. The Regions, the Province, the Ministry of Health and the Ministry of Labour have the possibility to access health data for governance purposes (as described in art. 12 paragraph 2 letter c) of Legislative Decree no. 179/2012 and by Articles 18 and 19 of Decree no. 178/2015). These data can be processed "as long as they are deprived of direct identification data of the patient and in accordance with the principles of indispensability, relevance and not excessive in relation to these purposes". In **Greece**, Law 4624/2019, Article 22 (paragraph 1b) implements the GDPR into Greek legislation and states that by way of derogation from Article 9 (1) of the GDPR, the processing of special categories of personal data, in the sense of Article 9 (1) of the GDPR by public authorities is allowed, if it is necessary for, among others: for reasons of preventive medicine, for the assessment of the employee's ability to work, for medical diagnosis, for providing health or social care or for the management of systems and health or social care services or potential contract with a

healthcare professional or other person bound by professional secrecy or is under his supervision. In **Sweden**, according to the Act (1998: 543) on health data registers, all health care providers are obliged to provide patient data to a health data register kept by the National board on Health and welfare, the Medical Products Agency and the Public Health Agency. But the purpose must be 1. Production of statistics, 2. Follow-up, evaluation and quality assurance of health care, or 3. Research and epidemiological investigations. In the **Netherlands**, the list is much more limited pertaining to the proper financial functioning of the health care systems and the data must be pseudonymised. **Romania** and the **UK** reported that in their country such specific legislation does not exist.

Country correspondents also reported the existence of legislation to allow secondary use of data for public health reasons. In **Poland** the legal regulations relating to the COVID-19 pandemic require that a positive test performed by a private entity must be reported to the Public Health Authority (Sanepid). In **Slovakia** the National Health Information Centre, a state funded organisation, maintains inter alia electronic records and national health registers and access is provided only to healthcare providers (under the Act No. 153/2004 Coll). Furthermore, in the case public health, such as tracing the source of infectious diseases, the Public Health Authority may use these data (under Act No. 355/2007 Coll). In **Hungary**, a similar system exists. Health and personal data from different sources can be connected only to the extent and for the period as it is necessary for the interests of prevention, treatment and public health or epidemiology purpose (under the Medical Data Act, section 10).

On the question whether this legislation also applied to non-healthcare providers, such as pharma or medical device companies, only Hungary answered positively, noting that the scope of their Medical Data Act includes every organisation which holds personal health data.

* *The Member State descriptions in this box serve as an illustration and are not exhaustive. The descriptions are based on the answers of an additional questionnaire that was responded to by a subset of countries.*

4.2.2. Health data sharing with insurers

Reimbursement within healthcare systems can be both to healthcare providers and to patients, depending on the nature of the healthcare system and the care being paid for. Such reimbursement demands that the payer knows what care has been provided. In a fully public system this could be per capita based payment, for certain types of routine care as well as payment on a named patient basis for specific services, such as vaccinations in a general practice context and in-patient care in hospital provided healthcare.

In order to explore the data protection aspects of health related data sharing with insurers further, the correspondents were asked to describe the situation in their Member State with respect to health data flow between healthcare providers and insurers. A summary of the responses is set out in Box 4.2 below.

Box 4.2 Examples: Providing health data to insurers*

Fifteen countries provided information on whether there is legislation which obliges a health care provider to release patient data to an insurer. Four countries reported that a defined data set has to be reported to the health insurers by the healthcare provider in order that the healthcare provider is reimbursed (Hungary, Croatia, Slovakia, and the Netherlands). Five countries reported not to have such an obligation (Italy, Malta, Poland, Romania, UK) while the remainder all noted that insurance contracts included specific consent about data releases and thus release to an insurer can only be made if such consent is shown. It may be surmised from this that if consent is not proven then the healthcare provider must refuse to provide patient data to an insurer.

A distinction must be made however between additional insurance taken out by a patient as a private contact and the insurance bodies which service the national health systems of Member

States. The responses provided for the UK and Sweden are good examples of how data release **to private or supplemental insurer** is handled:

- In the **UK**, under the General Medical Council confidentiality guidelines, a healthcare provider may refuse to disclose health data to insurers if the healthcare provider is not satisfied that: 1. the patient has sufficient information about the scope, purpose and likely consequences of the examination and disclosure, and the fact that relevant information cannot be concealed or withheld; 2. the healthcare provider has obtained or has seen written consent to the disclosure from the patient or a person properly authorised to act on the patient's behalf; 3. factual information cannot be substantiated or presented in an unbiased manner, which is relevant to the request; or 4. disclosing the information is not done with patient consent, cannot be justified in the public interest, and is not required by law.
- In **Sweden**, health data may only be shared with an insurer after the explicit consent of the patient. Furthermore, the Act (2006:351) on Genetic integrity prevents insurer from asking patients for granting access to genetic information. If the data may be withheld from the patient (see above under 2 b), it may also be withheld from insurers, even if the patient consents to the transfer of the data from the care provider to the insurer.

* *The Member State descriptions in this box serve as an illustration and are not exhaustive. The descriptions are based on the answers of an additional questionnaire that was responded to by a subset of countries.*

4.3. Market approval of medicines and devices

When discussing the use of health data for market approval of medicines and devices, such as medicines agencies, EMA, HTA and Notified Bodies, it is useful to bear in mind the following distinctions. The first is between market approval on the one hand and post marketing surveillance or pharmacovigilance on the other. The latter issue is addressed in the discussion under the next table. The other distinction is between who may collect the data for these distinct purposes under what circumstances. The bodies mentioned in Table 4.2 are allowed to access the original data or can retrieve those data when proper precautions have been met, for example in a pseudonymised form in a safe environment, which does not mean that they will not receive all data but only the data that was collected by others and then made accessible to those bodies in the context of a specific application.

Table 4.2 Legal basis for processing data that was originally collected for the purpose of providing care to allow it to be used for market approval of medicines and devices, such as medicines agencies, EMA, HTA and Notified Bodies.

Legal basis for market approval	Total MS	
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	7	BG, CZ, DK, IE, HR, IT, FI
6(1)(c) legal obligation + 9(2)(h) health or social care	3	BG, DK, HR
6(1)(f) legitimate interest + 9(2)(h) health or social care	0	
6(1)(e) public interest + 9(2)(h) health or social care	3	BG, DK, HR
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	4	BG, DK, FR, HR
Other combination	3	EE, FR, MT
No specific legislation	17	BE, DE, EL, ES, CY, LV, LT, LU, HU, NL, AT, PL, PT, RO, SI, SK, SE, [UK]

The fact that a variety of legal bases are cited, may suggest that the question was interpreted in different ways by different correspondents. It may be that some have read the question as asking how clinical trials or medical device clinical investigations are regulated, and hence who will collect the necessary data in that context for the market approval file. That will be industry. The question then is what legal basis is available under the GDPR for such data processing. Relating to clinical trials (which will soon be regulated under Regulation 536/2014/EU[10], hereinafter the CTR) a distinction must be made between data used for a trial and other data used for a market approval file, as set out by the European Commission in a Question and Answers document (COM, 2019a). According to the Commission's document under the CTR the mandatory aspects of the clinical trial file handling and reporting should be distinguished from 'pure' research activities. In the first case the GDPR legal basis for retention of data and reporting activities would be a legal obligation coupled with a public interest in the area of health laid down in EU law in the Clinical Trial Regulation (6(1)(c) and 9(2)(i) GDPR). In the case of 'pure' research activities, several legal bases might come into play. However, the distinction between the two types of data handling (compliance with trial reporting and 'pure' research) seems highly artificial as the activities are fully intertwined. Research in the context of a clinical trial is never purely for research purposes but always undertaken with an objective of submission to authorities, even if in some cases a trial is abandoned, and data are ultimately not submitted. This difficulty to distinguish between the clinical file handling and 'pure' research is reflected in some of the detailed answers of the country correspondents to the questions related to market approval of medicines and devices under the present clinical trial directive. For example, France answered that the processing of data collected in the context of clinical trials and according to the trial protocol is not based on consent in the sense of the GDPR. Of course, the (high) threshold for informed consent to participate in a trial must be met. It is yet another question whether the data collected in the context of a clinical trial may also be used for further research outside the protocol. In that case the GDPR and the national laws based on 9(2)(j) GDPR would apply (article 282 CTR). Others have interpreted the question as to be asking whether authorities can have access to data from the EHR's (and similar data from the primary function) or can get relevant pseudonymised data *in addition* to the market approval file as submitted by industry. That will also explain why respondents have answered that there is no such legislation.

The broad question also refers to HTA bodies (Health Technology Assessment bodies). Unlike notified bodies, medicine agencies or the EMA, there is no European legislation which prescribes that there should be HTA bodies and how HTA bodies will co-operate. Yet, they exist in many Member States and work together in a European network[11] introduced by Directive 2011/24/EU on the application of patients' rights in cross border health care. HTA is essential for sustainability of health care systems, yet their work is not without debate. Whether a specific treatment protocol is sufficiently effective to be reimbursed via the public health care system will often involve value judgements. HTA bodies can get their data from various sources, such as Cochrane reviews, scientific reports and specific observational studies which they have instated. In the comments to the tables, none of the respondents specifically discussed whether national HTA bodies can use data collected originally for care purposes. However, as such detailed data should generally be considered personal data regarding health, the HTA body would need a legal basis in 9(2)(h) or 9(2)(i) GDPR. This is for example the case for the HTA body

[10] Regulation EU No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/

[11] See https://ec.europa.eu/health/technology_assessment/overview_en

(NICE) in England.[12] In sum, based on section 251 of the NHS Act and then Regulation 5 pursuant to that Act, NICE can receive such centrally assembled data. The patient can opt out to the broad range of data uses based on Regulation 5. In the Netherlands, however the HTA body (ZiN-NL) would either have to rely on consent or a research exception in Dutch law (see the next Chapter) to collect data which are not anonymised.

4.4. Pharmacovigilance and medical device safety monitoring

Although pharmacovigilance is based on an EU directive (2010/84/EU), that directive does not state that personal data may be processed for this purpose. In the absence of Member State legislation allowing authorities or even pharmaceutical companies to process personal data for pharmacovigilance, these data need to be either fully anonymised or their processing based on consent. Some Member States have adopted legislation which grants the body to which adverse reactions must be notified a legal basis to process personal data concerning health in this respect. For example, the Danish respondent referred to the following relevant legislation: the (Danish) Medicines Act, The Act on Clinical Trials on Medicinal Products (will come into force when the CTR comes into force) and the Act on Medical Devices. These Acts include provisions authorising authorities to have direct access to personal data for monitoring medical device safety or pharmacovigilance and also provisions authorising the ministry to issue executive orders regarding duty of manufacturers, health authorities and licensed health care professionals to report malfunction, failure, deficiency and adverse events and reactions to the Danish Medicines Agency. In addition, the Health Act also includes a general obligation for all health care professionals to report adverse events to the Danish Patient Safety Authority. Reporting should include necessary information regarding the patients involved (personal identification number etc.), including necessary health information stored in medical files). The Irish system goes less far in requirements for the data which must be submitted but the Irish system does provide a legal basis for the body to which the reports must be sent, pursuant to Art. 9(2)(i) GDPR.

But other Member States, such as the Netherlands, while still implementing Directive 2010/84/EU have not adopted specific legislation clarifying the processing of data in such case. There is duty to notify to the central body but not exemption to professional secrecy that the physician may submit personal data for that purpose or that the body may process personal data concerning health. The legislation is older than the GDPR and usually has not been updated since. But also under the Data Protection Directive such a legal basis would have been necessary. Hence, in those countries such processing needs to be based on the consent or on anonymised data.

Just as for pharmaceuticals, Member States can take, and have taken, different routes concerning post market surveillance (PMS) and serious incidents with medical devices. As also for PMS for medical devices, soon to be fully regulated under Regulation 2017/745[13], there is no guidance on the EU level how such data can be collected at the national level. Devices makers do not know which device has been implanted into which patient and might have been taken out later, often by another health care provider, due to problems with the device. Regulation 2017/745 states in section 10 of article 87 that Member States shall take appropriate measures to encourage and enable health care professionals to report serious incidents with devices. Yet, problems with a device might

[12] Given the 'devolution' in the UK, formally NICE only applies to England. In practice its range is broader.

[13] Regulation 2017/435 EU 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

not be caused by the device. A reoperation might also be necessary because of problems caused during the initial operation, such as an infection. Serious incidents differ from possible indications which device works better for which patient, such as obese or not, still active or not. Fine grained information which can follow the patient with the implant over time is needed for real PMS which can explain variables in the performance of devices with sufficient unbiased external and internal validity, such as via case mix control. Given the fine grained data necessary for such registries, it cannot be easily assumed that those would necessarily be anonymous. If the data are to be useable for a recall they must retain a link to the patient, and therefore cannot be anonymous (see article 4.1 and recital 26 GDPR).

Some Member States, such as the Nordic countries and Greece have instituted systems for pharmacovigilance or PMS of devices, often via registries. Greece enacted legislation for patient registries in 2019. The establishment and operation of the registries is intended to defend, protect and promote the health of the population, through the planning and the implementation of public health policies, to ensure the universal and equal access to the providing of adequate in quality and in quantity health care services by the National Health System, to ensure the resources available for health care, to control expenditures and effective funding of health care, as well as to regulate the operation and the exercise of supervision over private health care providers.

But in other Member States such legislation does not exist. There may registries but in that case instituted bottom up without a statutory basis and hence navigating the consent or anonymisation approach. This explains the various legal bases mentioned in the questionnaire.

Table 4.3 Specific legislation adopted that addresses the processing of health data, used for monitoring of medical device safety and/or pharmacovigilance.

Legal basis medical device safety and pharmacovigilance	Total MS	
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	15	CZ, DK, DE, IE, EL, ES, FR, HR, IT, LV, LU, MT, AT, SI, FI
6(1)(c) legal obligation + 9(2)(h) healthcare	7	DK, DE, HR, LV, MT, AT, SI
6(1)(e) public interest + 9(2)(h) healthcare	5	DK, EE, EL, HR, LV
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	6	CZ, DK, EE, EL, HR, LV
6(1)(f) legitimate interest + 9(2)(h) healthcare	0	
Other combination	7	DE, EL, ES, FR, AT, PL, SE
No specific legislation	9	BE, BG, CY, LT, HU, NL, PT, RO, SK, [UK]

Looking at the literature on pharmacovigilance and PMS, Sethi (2014) provided an overview of the very divergent application of the then Data protection directive (95/46/EC) by Member States with regard to pharmaco-epidemiology. As seen in the answers to the questionnaire (see Table 4.3) but also in the OECD report of 2019 on using routinely collected data to inform pharmaceutical policies, the landscape is still very diverse (OECD 2019b). Sethi criticised the consent or anonymisation approach and the restrictions in many Member States to process and share personal data for pharmaco-epidemiology.

4.5. Public health threats

In the light of the COVID-19 pandemic, which was just peaking for the first time when the correspondents were working on the questionnaires, we asked several questions about re-use of data generated in the care context for disease reporting, tracking and tracing. The questions related directly to the wording in 9(2)(i) GDPR as well as to the WHO International Health Regulations (IHR). It should be noted however that the responses relate to reporting other than IHR compliant notifiable disease reporting, since all EU Member States have adopted IHR and implemented it into national legislation.

COVID-19 has demanded legislative speed and flexibility. Any public health system must have sufficient flexibility to add new legislation to respond to health threats. Yet the route taken might differ, based on different constitutional ordering of the Member States and traditions of public administration of the Member States. The report from France highlighted the enactment of special acts and presidential degrees in response to COVID-19 reporting. In the Netherlands, COVID-19 was added to the list of notifiable diseases by ministerial degree. Containing measures were left to the regional health authorities with a certain degree of central steering. Specific national COVID-19 legislation has been enacted only very recently and after lengthy debate in Dutch Parliament. In Greece a legislative act was published regarding measures in respone to Covid-19 pandemic, according to which the National Covid-19 Patient Registry was established, and later on, the above legislative act was specified by a Ministerial Decision.Noting the importance of timely disease reporting, the questionnaire asked if Member State level legislation allowed for data to be transmitted from the laboratories directly to institutions dealing with communicable diseases and/or ECDC, without going through a reporting cascade. It is interesting to note that the answers given here also shed more light on the answers given to the previous question. While some respondents mentioned horizontal data protection legislation in response to the previous question, here more details about the national public health system for transmissible diseases were given. The answers clarify that there is almost always some element of cascade as follows: from the health care provider or laboratory establishing the notifiable disease, the notification goes to the regional public health authority and from there to the national public health authority and from there to the ECDC. Yet, there are exceptions. E.g., in Denmark, an executive order can oblige laboratories to report cases directly to the national public health institute. In Ireland there is a national registry as will be discussed below.

Looking at this issue from the perspective of data protection, it will depend on Member State legislation when in that chain data will be anonymised. A regional health authority is traditionally primarily responsible for containment of individual cases. It knows the local circumstances and can perform the local research into the sources of the outbreak. It cannot do that without knowing the identity of the potential 'index patient'. It cannot order a specific person to self-quarantine or to submit to a treatment regime as an alternative[14] (if it has that authority[15]) if the identity of person is not notified to that authority. Depending on their role, the national authorities might simply gather statistics or need to know the pseudonymised data as well, for example to sort out multi reporting or to be able to give advice about the treatment or containment regime of a specific individual concerned. The national authorities will know when there are multi outbreaks

[14] Obviously not possible in the case of COVID-19. But there are other infections for which treatment is possible such as tuberculosis. Tuberculosis is still an important issue for public health authorities and its potentially devastating effects are only adverted because of this.

[15] In the Netherlands that authority is official higher up in hierarchy, namely the mayor of the place of resident of the infectious person, based on the advice of the public health authority.

and there is a need to scale up in preventive measures. The national authorities will be the 'competent bodies' in the sense of Regulation EC 851/2004[16] and will submit anonymised data to the European Centre for Disease Prevention and Control (ECDC). The ECDC has no mandate to receive data directly from laboratories or doctors finding a notifiable disease and the latter have no corresponding duty to submit such data to the ECDC.

In that respect a 'reporting cascade' is inevitable, unless there would be national databases where all notifiable cases are reported and which has to comply with the GDPR and professional secrecy as that may only in exceptional cases by overridden by public health threats. This will often depend on the implementation of a strict 'create, read, update and delete' or CRUD matrix based on roles and rights of the professionals. Only such systems can avoid a 'reporting cascade'. Ireland reported to have such a system, called Computerised Infectious Disease Reporting System (CIDR). The national public health institute can extract data from that system which can also be personal data insofar as necessary for their statutory function.

When there is no such centralised system and hence a 'cascade', the key question in terms of public health is more how speedily such a cascade can occur. There will be technical issues, in particular whether there is a fast electronic system for the exchange or that data from one layer have to be submitted manually to the other layer. From a regulatory perspective, legislation may require that the data from the layer where they have been initially collected is sent to the national public health institute directly, it may however also not specify this and leave more leeway to a local health authority to assess the situation first.

Here a distinction between notifiable diseases according to the IHR and other public health threats will be relevant. The various legal bases between threats not covered by the IHR and other threats such as sexually transmitted diseases, food borne illnesses and multi antibiotics resistant bacteria is shown in the following table.

Table 4.4 All EU MS are required to report diagnosis and outcome of the diseases covered by the WHO International Health Regulation, which now also includes COVID-19. Have MS enacted any national level specific legislation about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, which are not covered by the IHR?

Legal basis for protecting against serious cross-border threats	Total MS	
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	10	CZ, DE, IE, EL, LT, HU, PT, RO, SI, FI, [UK]
6(1)(c) legal obligation + 9(2)(h) healthcare	4	DE, EL, RO, SI
6(1)(e) public interest + 9(2)(h) healthcare	2	EE, RO
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	8	CZ, EE, IE, EL, MT, NL, RO, SI, [UK]
6(1)(f) legitimate interest + 9(2)(h) healthcare	0	
Other combination - please specify	0	
Not sure	1	PL
No specific legislation	12	BE, BG, ES, FR, HR, CY, LV, LU, MT, AT, SK, SE

[16] REGULATION (EC) No 851/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 April 2004 establishing a European centre for disease prevention and control.

The majority of the Member States answered that also other public health threats than those covered by the IHR will be notifiable and can be processed on the basis of 9(2)(i) GDPR (see Table 4.4). In some Member States they are not notifiable but the public health institute does have a legal basis to process such data. One Member State mentioned that the cooperation of the national public health institute with the ECDC around food- and waterborne diseases was not based on specific legislation but performed in the context of scientific cooperation. Hence the regulations for scientific research would apply. Though not explicitly mentioned by the other Member States, this will be the case for other situations as well where the pathogen is not listed yet in public health regulations as being notifiable.

4.6. Disease registries

The last questions discussed in this chapter relate to disease registries. The questions asked whether there is specific legislation to facilitate the creation and use of disease registries and if so, what legal basis is used. Here again we see a wide variation of possible legal bases. Multiple legal bases within one Member State can be explained by the fact certain registries are instituted by law while other registries are not. In Denmark and Sweden, for example, some disease registries are run by public health authorities, accordingly a national law under Article 6(1)(c) or (e) and 9(2)(h) or (i) GDPR will be applicable (see Table 4.5). For registries run by private data controllers, such as medical societies, the legal basis for processing would normally rely on the consent of patients. In France several registries operate under Article 6(1)(e) and 9(2)(i) GDPR; there is a specific recommendation of the French Data Protection Authority for cancer registries and rare disease registries, requiring that patients should be informed about the registry and have the option to opt-out. In countries where there is no specific legislation the registry will be based on either consent or on the national research legislation based on 9(2)(j) GDPR.

Table 4.5 Legal bases for processing data in disease registries.

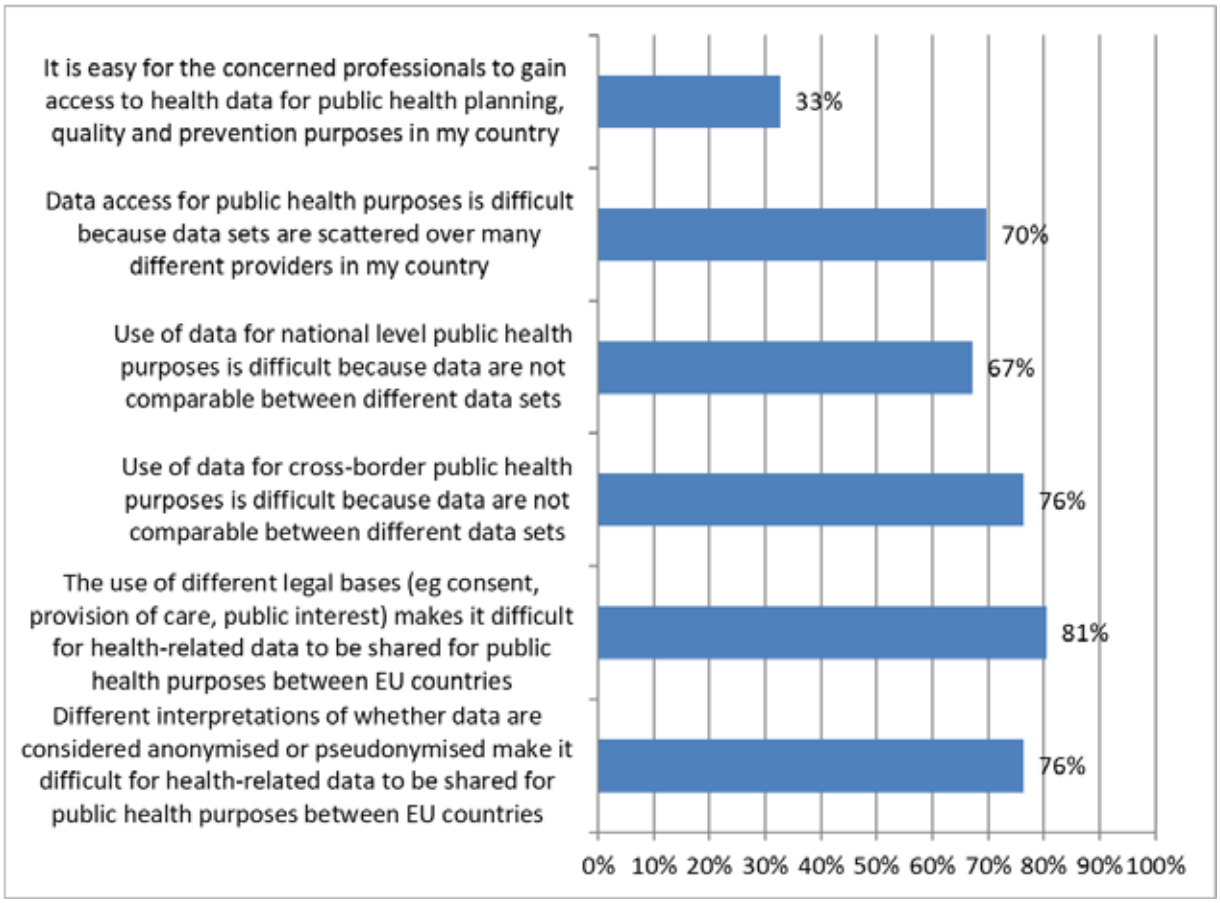
Legal basis for processing for disease registries	Total MS	
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	18	BE, BG, CZ, DK, DE, IE, EL, HR, LV, LT, LU, AT, PL, PT, RO, SI, SK, FI, [UK]
6(1)(c) legal obligation + 9(2)(h) healthcare	8	BE, DK, DE, EL, HR, LV, HU, SI
6(1)(e) public interest + 9(2)(h) healthcare	6	DK, HR, IT, LV, MT, SE
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	17	CZ, DK, DE, EE, IE, EL, ES, FR, HR, IT, LV, LT, MT, AT, RO, SK, SE, [UK]
6(1)(f) legitimate interest + 9(2)(h) healthcare	1	MT
Other combination	5	DK, DE, ES, IT, AT
No specific legislation	3	FR,CY, NL

In the EUROCOURSE project the case of cancer registries was explored in detail (Coebergh et al 2015). The legislation may have changed since then but the underlying idea of a 'registree' with strong roots in a community of stakeholders and carrying various fruits, from epidemiological surveillance to a reliable basic dataset for more advanced research remain the same. Majek et al showed the importance of registries for cervical screening programs (Majek et al 2019). Without monitoring their effects, a screening program becomes unreliable and cannot be justified anymore either. This would also apply to other (cancer) screening programs. Public screening programs depend on reliable epidemiological data which registries can provide.

4.7. Stakeholder views concerning processing of health data for public health purposes

The results of the stakeholder survey indicate very poor levels of access to health data for public health purposes. Most stakeholders agree that the use of different legal bases makes it difficult to share health data for public health purposes, but also show that other factors play a role, such as lack of comparability and scattered data sets over multiple providers (see Figure 4.1). Most stakeholders also indicated that relevant agencies should have easier and direct access and indicate that the EU should have a supporting role to facilitate this, for example by means of guidance or legislation.

Figure 4.1 Share of stakeholder agreeing with the following statements, all related to the way in which data sharing for public health purposes is possible

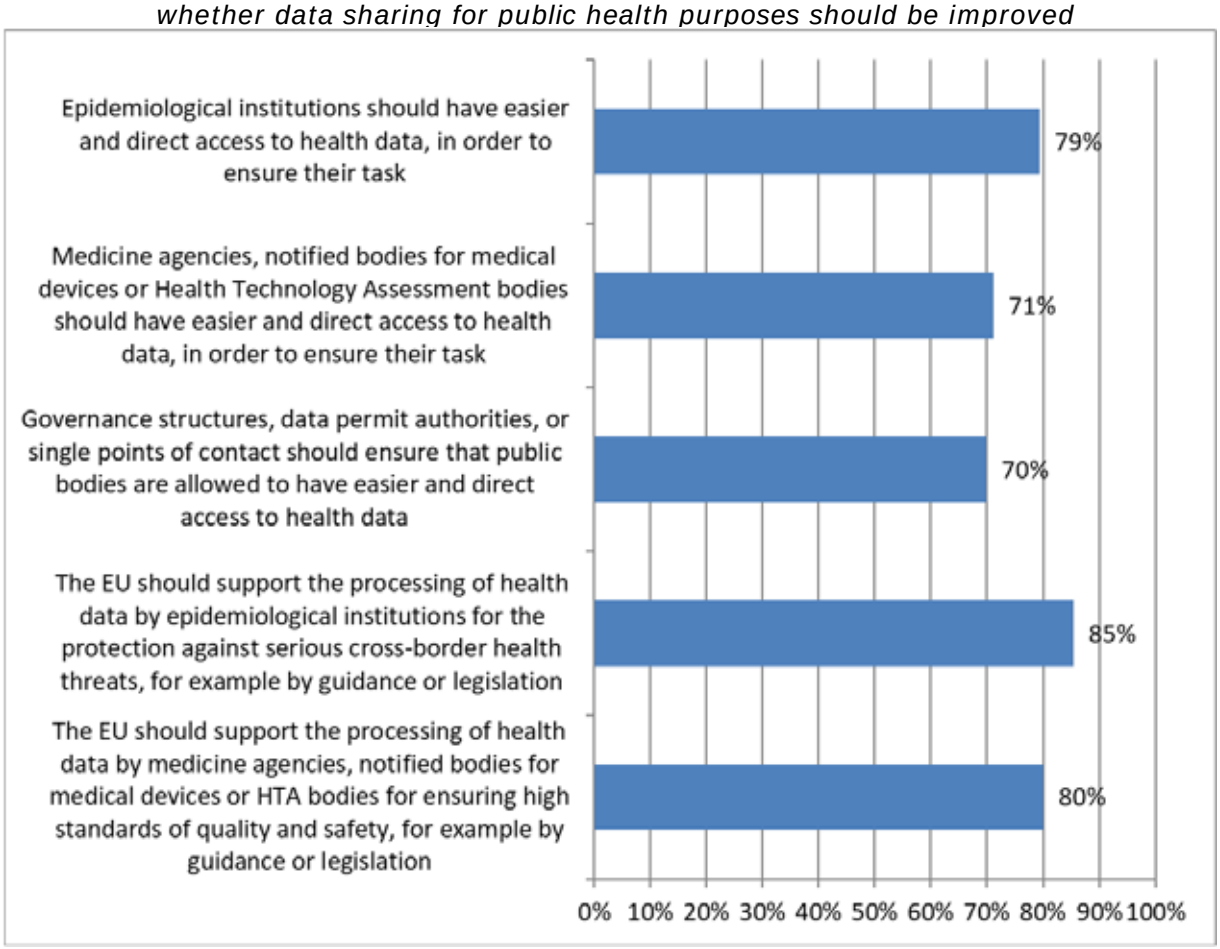


Relation with cross border health threats and COVID-19

The COVID-19 pandemic has significantly focussed attention on data sharing, both in the context of public health reporting of disease incidence and contact tracing, and on the need for accessible data for collaborative research across many countries, both within and beyond the EU. This is also reflected in the views of stakeholders on the online survey, as displayed in Figure 4.2. The onset of the pandemic has made it even more necessary to rethink the availability and accessibility of data. Not surprisingly, COVID-19 was also discussed extensively during the workshops, as it was widely acknowledged that health data are needed in the fight against the virus and the protection against serious cross-border health threats in general. Here again a fragmentation of approaches has been noted, as not all Member States seemed to have implemented national level legislation to address the use of data for the management of serious cross-border health threats as provided for in Article 9(2)(i). However, the guidance adopted by the EDPB (2020b) in the context of COVID-19 has gone some way towards driving a more

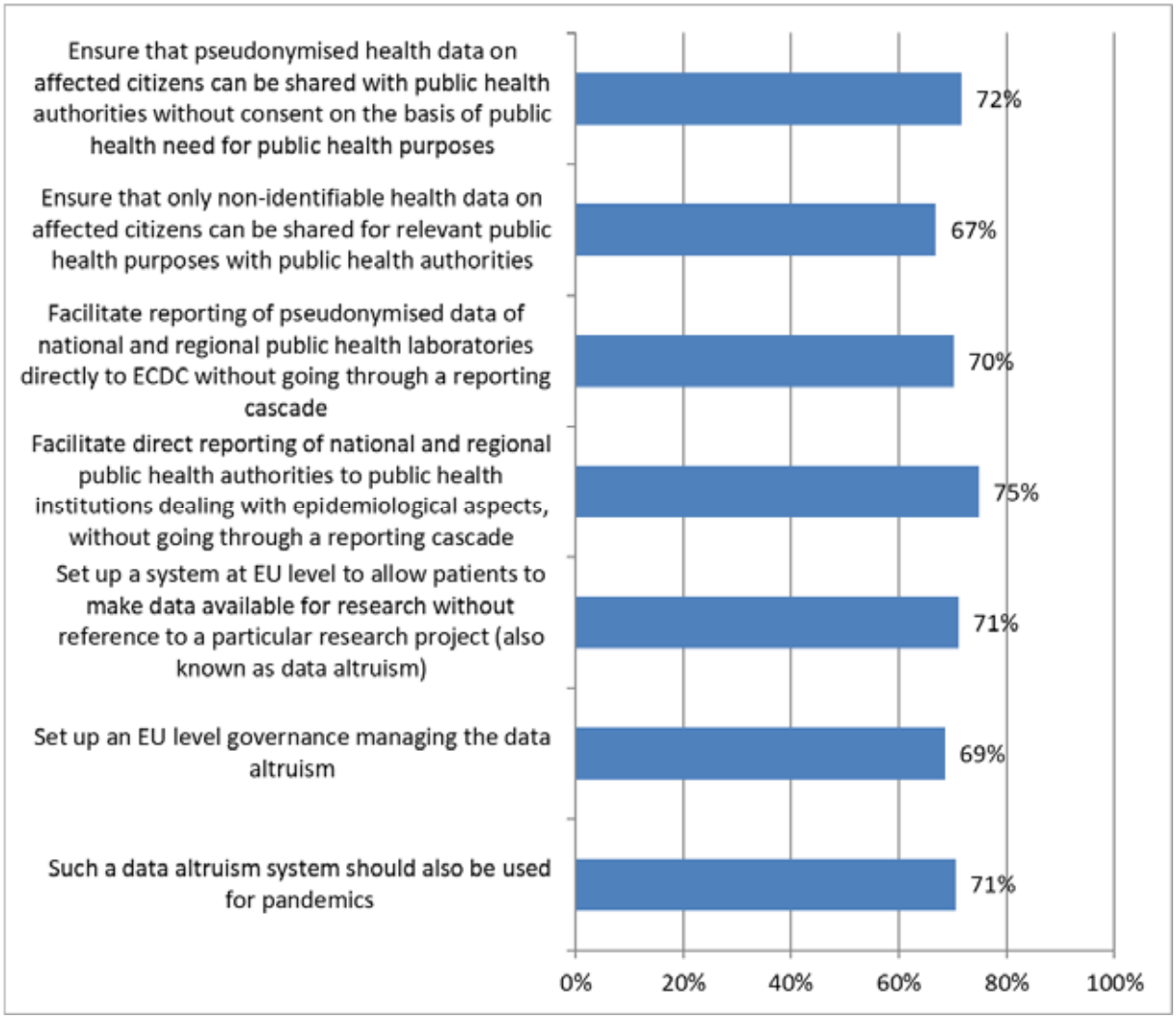
consistent interpretation and approach to the application of GDPR on health data processing, as well as on health data research.

Figure 4.2 Share of stakeholder agreeing with the following statements, all related to whether data sharing for public health purposes should be improved



It was noted also that data sharing with the ECDC or the WHO to facilitate aggregation of data at European level is not as smooth as it might be. The issues here were however not only attributed to variations in interpretation of EU law, but also to more practical issues, such as the lack of a uniform reporting methodology and very limited datasets reported to ECDC. Stakeholder audiences indicated that the use of (pseudonymised) health data should be improved for public health purposes, and there was also support for a data altruism approach when dealing with a pandemic (Figure 4.3). Workshop participants reported challenges arising from lack of interoperability of health data and accordingly the need for more EU level guidance. Reference was also made to the need for a balance between fundamental human rights and freedoms with the need to respond to a virus, requiring adequate mechanisms with the right checks and balances to avoid becoming a surveillance society, in line with current debate in many Member States on the use of technologies such as geolocation, immunity passports and infrared cameras and the discriminatory risk they may have.

Figure 4.3 Share of stakeholder agreeing with the following statements, all related to the way in which responses to future communicable disease outbreaks should be improved



4.8. Concluding remarks

The wide range of answers to questions shows some common denominators, but many variances as well. In nearly all Member States there is national law for data processing in function 2 in accordance with Article 6(1)(c) or (e) GDPR and Articles 9(2)(h) or 9(2)(i) GDPR. Yet there seem to be huge differences between Member States regarding how PMS is organised, both for medicines and devices. The same applies to access for HTA bodies and to disease registries. Access - if any - to personal data for each of these functions is usually fragmented over a variety of Acts and decrees which have been enacted over time, and follows different guidance of Data Protection Authorities. Though as a whole such legislation should be coherent, no Member State was reported as having one central body which can give access to data in all the various source databases (EHR's, industry data, health insurers data, etc.) for public health purposes. As is shown from the stakeholder survey many feel that access for public health purposes is not only fragmented but also insufficient. The recently developed data permit authorities in Finland and France will in due course provide such a coherent reference point for those countries, but full access to all health data sources was not reported for those countries in this study.

The discussion on responses to COVID-19 shows that more attention is needed on the role of law in ensuring sharing of data to facilitate the timely identification of new trends in public health threats. None of the respondents answered that EU bodies such as the EMA or ECDC have direct access to data relevant for their mission, and as such identify the need for further EU level regulation to support public health objectives at EU level. The impact of the heterogeneity of the present national systems is reflected also in the responses of stakeholders. The vast majority do not seem happy with how the present system functions, and seem to see little evidence of any form of coherent EU wide system, while some stakeholders also relate dissatisfaction with Member State level possibilities for further processing of health data for public health purposes.

As noted in chapter 3, the GDPR foresees a role for further EU level legislation as well as national level legislation to address these issues, in line with the Treaties. The rising demand on healthcare systems, driven by ageing populations as well as novel health threats such as the coronavirus could provide the required interest among member states to explore further legislative option. Furthermore, the rise in new technological advances, including artificial intelligence, which are dependent on access to large quantities of data will serve as an important impetus to EU level action to facilitate better use of data to ensure that Europe's healthcare systems can be resilient and that the EU can establish its place as a world class player in the development of new health technologies.

5. SECONDARY USE OF HEALTH DATA FOR SCIENTIFIC OR HISTORICAL RESEARCH

5.1. Introduction: defining function 3 and the legal basis for secondary use of health data for scientific research

The legal framework for secondary use of health data for scientific or historical research (Function 3) is addressed in this chapter. **Function 3** concerns data processing for scientific or historical research by both public and private sector organisations (third parties, not being the original data controller), including the pharmaceutical and medical technology industries and insurance providers. This, together with function 2 (see Chapter 4), is generally referred to as a **secondary use**. The secondary use examined in this chapter concerns public research entities (including universities, public health laboratories) and private sector entities. These entities may use data that remain stored within primary use repositories, such as Electronic Health Records (EHR) systems, but may also be brought together in other systems such as disease **registries** which collect data to calculate disease incidence and prevalence at **national or regional level.**

5.1.1. Legal basis for processing -function 3- research

This chapter concerns the governance of personal health data collected in the context of providing care which are subsequently re-used for research purposes. Such use may be conducted by public sector organisations, publicly funded researchers, researchers based in not for profit organisations and researchers based in industry such as commercial research organisations or other privately funded research organisations.

As the focus of the chapter is the re-use of health data, it is important to understand the difference between primary and secondary use in research. There are two types of data usage when it comes to "processing of health data for the purpose of scientific research":

1. Research on personal health data which consists of the use of data directly collected for the purpose of scientific studies ("primary use");
2. Research on personal health data which consists of the further processing of data initially collected for another purpose ("secondary use").

It is worth noting that the terminology can be confusing, as in this report the term primary use is also used to refer to the use of health data for care, known in this report as function 1.

In accordance with Article 6(4) GDPR, data can only be further processed for a purpose other than the purpose stated at the time of collection if it is compatible with that purpose (known as the purpose limitation principle). When it comes to research however, this should be read in conjunction with Article 5(1)(b) which carves out a privileged position for research, stating that further processing for scientific research purposes in accordance with Article 89(1) is not considered incompatible with the principle purpose. However, it should be borne in mind that the EDPS, building on recital 159 of the GDPR, makes a distinction between 'genuine research' and other research in this respect (EDPS 2020). That distinction is important. Research should meet methodological requirements, standards of research integrity (KNAW 2018), and aim to contribute to the common good. Given the respondents and the regulations which are referred to in this chapter, the research discussed here falls into that category of genuine research.

5.1.2. Lawful bases and safeguards

The GDPR permits processing of health data for research purposes where one of the lawful bases set out in Article 6(1) applies and the data controller can also meet one of the relevant derogations in Article 9(2), otherwise the processing of special categories of data such as health and genetic data is prohibited (see Box 5.1).

Box 5. 1 Article 9(2) GDPR – condition of processing "special categories" of data and Article 89(1) safeguards

Article 9(1) notes that in general processing of data concerning health or genetic data shall be prohibited. Article 9(2)(a) provides that this prohibition will not apply if the data subject has given **explicit consent**, unless Member State law states that the prohibition in 9(1) cannot be lifted by explicit consent. This is the case in some EU countries for genetic tests or other specific medical examinations (van Veen, 2018).

As seen, the GDPR allows for exceptions to the principle of explicit consent, usually if based on national or EU legislation. The following may be applicable for secondary processing of health related data for research in the context of:

- 9(2)(b) carrying out duties under social employment and security law as set out in Member State or Union law - note this may apply to healthcare data processing for research by public sector bodies in some Member States where the administration of healthcare services is set out within wider social security law;
- 9(2)(c) necessary to protect the vital interests of the individual;
- 9(2)(h): processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- 9(2)(i): processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- 9(2)(j): processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The GDPR provides that Member State legislators may adopt legislation to allow for use of data for research in accordance with Article 9(2)(j) and 89(1)). It is clear from the responses provided by the correspondents that the Member States have not implemented such legislation in a homogenous way, resulting in a complex and fragmented landscape for researchers to navigate. Consequently, differences between Member States in the way the GDPR is implemented and interpreted in the area of scientific research has made data exchange between Member State and EU bodies for research purposes difficult and in some cases highly technical.

Variation also exists between Member States in how they distinguish between public and non-public sector researchers. This is relevant as the definition can influence the selection of lawful basis. As pointed out by participants in the workshops, the distinction between public and non-public research is not always clear-cut, and many hybrid forms exist, notably when commercial organisations provide unrestricted grants for research conducted in public universities.

This is relevant because in addition to relying on the provision for scientific research in Article 9(2)(j) certain categories of researchers may also be able to rely on Article 9 (2)(i) where research is in the public interest. This will however be difficult for researchers in for-profit organisations who may find it challenging to prove that research is in the public interest.

The public interest legal basis can only be invoked where such processing is provided for in Member State or EU law. This will demand that the legislator defines which type of researchers may make use of the public interest criterion. It will also demand that the legislator has weighted the risks to the individual against public benefits. One such balance test applied in the context of research has been called the 'duty of easy rescue' test (Porsdam Mann et al 2018). The 'duty of easy rescue' may be described as arising when it is possible to benefit others at no or minimal cost to oneself. Porsdam Mann et al argue that where the duty of easy rescue does not apply because there are significant risks involved in data sharing and where these risks cannot be minimized by security management, research can only ethically proceed without informed consent when obtaining consent would be impossible or impracticable, the public benefit of the research very significantly outweighs the risks, the public is adequately informed, and any resulting harms are compensated. These balances as described have however not yet been developed into easily applicable criteria in national or EU level law (Schaefer et al 2020) which adds further complexities.

This study seeks to examine and analyse the legal patchwork and technical burdens which have emerged across Member States in particular looking at Article 89(1) safeguards for research and lawful bases as provided for in the GDPR.

5.2. Survey findings: legal bases used to legitimate processing of health data for Function 3 - Research

5.2.1. Introduction to findings

This section reports on the outcomes of the two surveys as described in chapter 2 - one survey completed by national level expert correspondents, and one stakeholder survey completed as an online survey sent to a wide range of stakeholders. The findings of both surveys are complemented by a series of workshops held between February and June 2020. Both the legal and stakeholder surveys asked a range of questions on four situations in which data are processed within Function 3:

- A number of questions **about legislation which addresses the re-use of health data for research;**
- A number of questions concern research conducted by the **healthcare professional who originally collected** the data for the purposes of treating the patient;
- A number of questions concern research conducted by **third party researchers**, including public sector or publicly funded researchers, researchers based in not for profit organisations and researchers based in industry or commercial research organisations other privately funded research organisations;
- A number of questions concerns research by any type of organisation on **genetic data.**

5.2.2. *Findings - sectoral legislation or authoritative guidance further specifying the application of article 9(2)(j) in the context of health research*

As already stated, Article 5(1)(b) indicates that further processing of data for scientific or historical research purposes is not to be considered incompatible with the purpose limitation principle if processing is undertaken with suitable safeguards in accordance with Article 89(1). The legal survey asked whether Member States adopted sectoral legislation or authoritative guidance, in the context of the implementation of Article 9(2)(j), which further specifies the application of this article in the context of health research.

The results of the legal survey indicate that 9 Member States were reported as not having adopted sectoral legislation. Of the 18 Member States who were reported as having such legislation, there are variances in safeguards applied (see Table 5.1). Where a Member State is listed as not having sectoral legislation in place to address the use of data for research, this does not imply that data cannot be used in line with Article 9(2)(j) at all, it may mean that the provisions for such use are included in the general data protection legislation that has been implemented in pursuance of the GDPR. In Ireland, for example, the Data Protection Act 2018 provides a large number of justifications under Art. 9(2) GDPR laying down derogations for processing health data, including for scientific research. Accordingly a researcher may need to refer to general data protection law, sectoral law, and may also need to read such laws alongside authoritative guidance which addresses use of data for research; similarly Ireland has adopted a statutory instrument, the Health Regulations 2018 which further defines the provision in Section 36(2) of the Data Protection Act.

Table 5.1 Sectoral legislation or authoritative guidance by Member States in the context of article 89

Member State has adopted sectoral legislation or authoritative guidance specifying safeguards to be applied in line with Art. 89 in the context of health research	**Total MS**	
No	9	CZ, FR, CY, LT, HU, NL, PL, PT, SK
Yes	18	BE, BG, DK, DE, EE, IE, EL, ES, HR, IT, LV, LU, MT, AT, RO, SI, FI, SE, [UK]
If yes, the following issues are addressed specifically in that legislation		
Scientific research by public sector organisations	12	BG, DK, DE, EE, EL, ES, HR, LU, MT, AT, FI, SE
Scientific research by private sector organisations	9	DK, DE, EE, ES, LU, MT, AT, FI, SE
Research for development of national statistics	12	BG, DK, DE, EE, EL, ES, HR, LU, MT, AT, RO, FI
Research for authorities' planning	9	BG, DE, EE, ES, HR, LU, MT, RO, FI
Other, please explain	6	BE, IE, ES, IT, LV, RO, [UK]

Pseudonymisation and anonymisation

Article 9(2)(j) GDPR requires that Member State or EU law which provides for the processing of sensitive data for scientific research purposes in accordance with Article 89(1) shall include the use of suitable and specific measures to safeguard the fundamental rights and interests of the data subject. Article 89(1) holds that safeguards shall ensure technical and organisational measures are in place to uphold the principle of data minimisation and goes on to highlight some measures which may be used to

achieve this principle such as pseudonymisation or anonymisation. Further guidance is given in Recitals 156-163.

One of the safeguards most relevant to health sector research is pseudonymisation. This is cited by the GDPR as a mechanism for protecting data when the data to be re-processed cannot be anonymised. Here again, variation arises between the Member States, not only because of particular differences in the standards for pseudonymisation, but also because of different interpretations at national level.

When referring to anonymisation Recital 26 notes that in determining if data are anonymous, account should be taken of all means reasonably likely to be used either by the controller or by another person to identify the individual from the data, such as the cost and time required for identification, taking into consideration available technology at the time of the processing and technological developments. Data that has been anonymised is no longer considered personal data.

Divergence arises between Member States as to what are considered "tools" likely to be used to identify individuals. In workshop discussions it was noted that in practice some Member State authorities work on the basis that full anonymity can never be achieved for health-related data while still keeping the data useful for research, others believe anonymity within the meaning of GDPR can be achieved. In the literature it was noted that anonymous data, to the highest standards without any residual risk for re-identification, may lose their value for nuanced research (Van Veen, 2018, Mondschein and Monda 2019). Similar differences in interpretation also exist with respect to pseudonymisation (Article 4(5) GDPR). The legal definition of pseudonymisation under the GDPR is quite far-ranging (Mourby, 2018, see also Groos and van Veen, 2020). As a result, a number of misconceptions have arisen as to its meaning. This issue was addressed by the Article 29 Data Protection Working Party, who note that pseudonymised data cannot be considered equivalent to anonymised data "as they continue to allow an individual data subject to be singled out and linkable across different data sets. Pseudonymity is likely to allow for identifiability, and therefore stays inside the scope of the legal regime of data protection. This is especially relevant in the context of scientific, statistical or historical research" (Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 2014). Yet, some authors criticize the approach in that Opinion and nuance its all or nothing approach especially after the Breyer decision of Court of Justice (C-582/14, ECLI:EU:C:2016:779) which according to those author calls for a more contextual approach (Groos and van Veen 2020 with further references).

Member State application of safeguards

Taking these difficulties in interpretation into account, it is worthwhile to note some of the examples from national legislation provided by the experts in response to this question (Box 5.2-5.5): *Has your Member State adopted sectoral legislation or authoritative guidance which in the context of the implementation of Article 9(2)(j) further specifies the application of this Article, further processing Article 5(b) & Article 89(1)) in the context of health research*?

Box 5.2 Estonia - Personal Data Protection Act

Chapter 2, Paragraph 6- Processing of personal data for needs of scientific and historical research and official statistics

(1) Personal data may be processed **without the consent** of the data subject for the needs of scientific and historical research and official statistic, in particular in **a pseudonymised format or a format which provides equivalent level of protection**. Prior to transmission of personal data for processing for the needs of scientific and historical research or official statistics, personal data shall be replaced by pseudonymised data or data in a format which provides equivalent level of data protection.

(2) De-pseudonymisation or **any other method** by which the data not enabling identification of persons are changed again into the data **which enable identification of persons are only permitted for the needs of additional scientific and historical research or official statistics**. Processors of personal data shall designate a person identified by name who has access to the information allowing pseudonymisation.

(3) Processing of data concerning any d**ata subjects for the needs of scientific and historical research or official statistics without the consent of the data subject** in a format which enables identification of the data subject is permitted only in the case the following conditions are met: 1) **the purposes of data processing can no longer be achieved** after removal of the data enabling identification or it would be unreasonably difficult to achieve these purposes; 2) there is **overriding public interest** for it in the estimation of the persons conducting scientific and historical research or compiling official statistics; 3) the **scope of obligations** of the data subject is not changed based on the processed personal data or the rights of the data subject are not excessively damaged in any other manner.

(4) If scientific and historical research is based on **special categories of personal data**, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate.

Box 5.3 Germany- Federal Data Protection Act – BDSG- Section 22 § 2 sentence 2 in conjunction with Section 27 § 1, sentence 2 - special categories of data

Federal law:

Section 27 (1) BDSG:

By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research purposes or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

§ 22 II BDSG:

In the cases of subsection 1 [permission for the processing of special categories of personal data], appropriate and specific measures shall be taken to safeguard the interests of the data subject.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

1. **Technical organisational measures** to ensure that processing complies with the GDPR;

2. Measures to ensure that it is subsequently possible to **verify and establish** whether and by whom personal data were input, altered or removed;

3. Measures to **increase awareness of staff involved** in processing operations;

4. Designation of a **data protection officer**;

5. Restrictions on access to personal data within the controller and by processors;

6. The **pseudonymisation** of personal data;

7. The **encryption** of personal data;

8. Measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;

9. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

10. Specific rules of procedure to ensure compliance with this Act and with the GDPR in the event of transfer or processing for other purposes.

(Note: regulation in the federal states on health research)

Box 5.4 Spain - Additional Provision 17a.2 of the Organic Law 3/2018, of 5 December 2018 of Protection of Personal Data and guarantee of digital rights

Spanish national law further specifies the rules for processing health data collected for research purposes, these include:

- **Health authorities and public institutions** with competences in **public health surveillance** may carry out scientific studies **without the consent** of the data subject in **situations of exceptional relevance and seriousness for public health.**
- **The re-use of personal data** for biomedical research purposes will be considered lawful and compatible when, **having obtained consent for a specific purpose,** the data is used for purposes or areas of research related to the area in which the initial study was scientifically integrated. In such cases, the persons responsible must publish the information established by Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in an easily accessible place on the corporate website of the centre where the research or clinical study is carried out and, where appropriate, on the website of the sponsor, and notify the persons concerned of the existence of this information by electronic means. When the subjects do not have the means to access this information, they may request that it be sent in another format.
- The **use of pseudonymised personal data for research in biomedical research is considered to be lawful**. The use of pseudonymised personal data for biomedical research purposes will require: 1. A technical and functional separation between the research team and those who perform the pseudonymisation and keep the information that makes re-identification possible: 2. That the pseudonymised data is only accessible to the research team when: i) There is an express commitment to confidentiality and not to carry out any re-identification activity. ii) Specific security measures are adopted to prevent re-identification and access by unauthorized third parties. Re-identification of data at origin may take place when, in the course of an research using pseudonymised data, it becomes apparent that there is a real and specific danger to the safety or health of a person or group of persons, or a serious threat to their rights, or that it is necessary to ensure proper health care.
- The use of **pseudonymised personal data for research purposes must be subject to the prior approval of the Research Ethics Committee**

Box 5.5 Denmark - Act no. 502 of 23/05/18

In Denmark, Articles 9(2)(j) and 89 GDPR have been 'activated' in section 10 of the Act no. 502 of 23/05/18 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

Section 10 allows for processing of personal data **without the data subject's consent** for the sole **purpose of carrying out statistical or scientific studies** of significant importance to society and provided such processing is necessary in order to carry out these studies. A number of **supplementary conditions apply**. First of all, according to section 10.2 of the Data Protection Act, personal data collected for scientific or statistical purposes based on Article 10(1) may not be used for other purposes. However, Article 10(5) of the Act gives the **Minister of Health (after consultation with the Minister of Justice) authority** to issue binding rules (executive orders) regarding exemptions from Article 10(2) in situation where vital interests of the data subject speak in favour of this. According to the preparatory work this exemption is introduced to ensure the vital interests of the data subject in situations where a health research project or statistical analyses reveals a specific risk of having a serious disorder (including genetic disorder) for which prevention or treatment is available. This could also include situations where data is processed as a support for making clinical decisions regarding provision of personalised/precision medicine. It is anticipated that rules, which will be issued based on section 10.4, will include safeguards to ensure proper respect for the data subjects interests and rights. If data are to be transferred to a third party outside the EEA, permission from the Danish Data Protection Authority is needed (section 10.3). This is also the case if transfer involves human tissues samples (also with the scope of the GDPR), or the transfer of data serves the purpose of publication in a recognized scientific journal or similar.

Apart from the Data Protection Act, the Health Act also has a few provisions regarding use of health data for research purposes. Section 46.1 of the Health Act, allows for further use of data from health records and registers for scientific purposes, provided the project has been **approved by a Research Ethics Committee (REC)**. If the project is not approved by a REC, which will be the case for most projects which are exclusively based on personal data, the **Regional Council** must authorize access to the data subject's health records (section 46.2 of the Health Act. It is a condition that the project has **significant societal interest**, and the **Patient Safety Authority** can lay down further conditions for the processing of the data. It is furthermore a condition, that the **data subject can only be contacted with the permission of the health care professional, who has provided the treatment** (section 46.3). Finally, the data may only be processed for scientific purposes, and any publication of the data must ensure that the data subject is not identifiable (section 48).

These examples highlight the different regimes for secondary processing across Member States. Some Member States adopted legislation, others authoritative guidance and some nothing. Pseudonymisation is a common requirement with other safeguards ranging from Research Ethics Committee approval, appointment of a data protection officer, to technical and organisational measures ensuring compliance with GDPR (see also Box 5.6 for a more detailed description for a number of examples).

Box 5.6 Some examples of sectoral laws which address the release of patient data for research purposes*

Fifteen countries provided additional information on the existence and content of sectoral laws concerning the release of patient data for research purposes. Three Member States reported to not have such laws (Romania, Slovakia and Sweden). Eleven Member States have such legislation in place (Bulgaria, Croatia, Denmark, Greece, Hungary, Ireland, Italy, Lithuania, Malta, the Netherlands, Poland [and the UK]).

In **Bulgaria**, the National Centre of Public Health and Analyses (NCPHA), for example uses health data in relation to its work on public health protection, health promotion and disease prevention, information security management of healthcare. The information is de-identified. The NCPHA manages, controls, monitors and coordinates health information activities, such as:

- Developing and unifying the medico-statistical documentation about the health status of the population and about the resources and activities of the medical establishments;
- Developing mathematical models and plausible forecasts for demographic trends and health status of the population; provides practicable and annual medico-statistical and economic information;
- Carrying out activities for the development of a unified health information system and eHealth;
- Developing and implementing a patient classification system and reporting and payment technologies;
- Maintaining classifications, nomenclature, standards and methodologies;
- Participating in the implementation of statistical activities of the state in cooperation with the National Statistical Institute; maintains, updates and publishes health information standards;
- Organising, coordinating and controlling eHealth development activities; develops methodologies and models for resource planning and management for healthcare facilities;
- Developing, implementing and maintaining national coding standards in healthcare settings and monitors the coding process.

In **Croatia**, according to Article 5.2, further processing of health data is allowed for archiving purposes in the public interest, for the purposes of scientific or historical research or for statistical purposes for the purpose of studying and monitoring the state of health of the population or for other purposes determined by special law. The Act does not regulate obligation to obtain an ethical committee approval. Each Data controller has its own Ethical committee which is deciding on approval upon each submitted request for the release of patient data for research purposes.

In **Greece**, Article 84 (4) (4c) of Law 4600/2019 states that sensitive personal data collected and further processed in the context of the Individual Electronic Health Record, in accordance with the provisions of this Regulation, is exceptionally permitted to be processed, if, among others the processing is necessary for archiving purposes on the grounds of public interest, for scientific or historical research purposes or for statistical purposes, in accordance with paragraph 1 of Article 89 of the GDPR, under European Union law or national regulations, for purposes which are analogous to the intended purpose, which respect the essence of the right to data protection and which provide appropriate and specific measures to safeguard the fundamental rights and interests of the data subject. Also, article 83 (3) (f) states that the processing of the data, collected and processed in the context of the National Patients Registry is allowed, if, among others, processing is necessary for archiving purposes on grounds of public interest, for scientific or historical research purposes or for statistical purposes, in accordance with paragraph 1 of Article 89 of the General Data Protection Regulation, and with the European Union law or national regulations, which are analogous to the intended purpose, respect the essence of the right to data protection and provide appropriate and specific measures to safeguard fundamental rights and interests of the data subject.

- Covid-19 Patient Registry (Joint Ministerial Decision 2650/2020), Article 4 par. 9 states that patients' personal data, which are part of the archiving system of the National Patient COVID-19 Registry are kept until patient's death and for twenty years after patient's death. This information may, after patient's death, be stored indefinitely, using pseudonymization and / or encryption techniques, provided that it is processed only for the purposes of managing the health and social systems and services specified in Article 9 (2). 2 items (h) of the GDPR, as well as for archiving purposes for the public interest, for the purposes of

scientific or historical research or for statistical purposes, in accordance with Article 89 par. 1 of the GDPR.

- Law 4712/2020, Article 77: Regulations regarding the emblematic action to tackle the virus SARS - Cov-2 states that research centers "participating in the Emblematic Research Action for the treatment of the virus have access to positive samples from all laboratories diagnosing a patient infected with the SARS-Cov-2 virus and included in the National Patient Registry for COVID 19 in order to perform virome analysis and to confirm the diagnosis by immunological methods. In case of scientific research, the patient is informed and informed consent must be obtained.

In **Ireland**, according to the Health Research Regulations 2018 section 3 (1) (b) (1) a research project must have Research Ethics Approval.

Italy distinguishes three different situations:

- Data within the Fascicolo Sanitario Elettronico (FSE): D.l. 179/2012 is the national legislation establishing the "Fascicolo Sanitario Elettronico" (henceforth: FSE), whose rules of functioning are further specified in DPCM 178/2015. FSEs are electronic health records that collect and bring together, in a single electronic file, all the medical information that regard a specific citizen (such as medical records, prescriptions, etc.). This information is collected in every interaction that the assisted person has with healthcare providers and professionals accredited within the national health service. FSE data can be accessed for research and government purposes, without the consent of data subject, upon request to the data controllers (the Region that has established the FSE and the Italian Ministry of Health). For example, in the case of the FSE set up by the Lombardy Region, the FSE (without directly identifying data) may be used for medical and epidemiological research purposes (provided for by law, by a biomedical and health research program or authorized by the DPA) by the Lombardy Region and the Ministry of Health (data controllers). A specific consent will be required to use FSE data for research projects other than those mentioned above.
- Data within registries**:** Law 29/2019 establishes and regulates the National Network of Cancer Registries and Surveillance Systems and the Epidemiological Report for the health control of the population. Art. 1.6 of L. 29/2019 allows the Ministry of Health, upon prior consultation with the Italian DPA, to sign cooperation agreements (free of charge) with universities, public and private research centres, and other scientific organisations, for the processing of data contained in the National Network**,** provided that such entities: i) have been involved for at least ten years in a not-for-profit manner in activities such as, among others, accreditation of cancer detection systems according to national and international standards, and development of national databases; ii) pursue their activities on the basis of codes of conduct ensuring transparency and the absence of conflicts of interests. Art. 2.1 of L. 29/2019 allows the Ministry of Health, upon prior consultation with the Italian DPA, to reach cooperation agreements (free of charge) with third sector entities, such as oncologic associations, for the processing of data contained in the National Network, provided that such entities: i) pursue their activities on the basis of codes of conduct ensuring transparency and the absence of conflict of interests; ii) appoint a scientific committee composed of experts in tumour epidemiology and in oncology, as well as at least one representative of a tumour registry, tasked with ensuring that the information conveyed is based on robust scientific and epidemiological standards. The purposes for which data from the National Network can be processed are outlined in Art. 1.1 of L. 29/2019, and include prevention, epidemiological control, promotion of scientific research in the oncological domain, etc. Pursuant to art. 1.2 of this legislation, the Ministry of Health should issue, by April 2020, a regulation clarifying the specific modalities of the data processing and the subjects that will be allowed to access the National Network. NB: At the time of writing, this regulation has yet to be issued.
- Data collected by healthcare **providers for the purpose of care:** Here, the healthcare provider is entitled to make agreements with third party researchers in order to transfer patients' data for which consent has been provided. In addition, the processing of personal data for research is bound to EU (GDPR) and national data protection requirements. In particular, within the Italian Data Protection Code, Title V concerns specific provisions for the "Processing of personal data in the health domain", while Title VII concerns specific provisions

for the "Processing for archiving purposes in the public interest, scientific or historical research or for statistical purposes". The articles comprised within Title V (from 75 to 93) concern general principles underpinning health data processing, the ways to inform data subjects and provide the privacy notice, the way to deal with prescriptions, medical records, and the certificate of childbirth assistance. The articles comprised within Title VII (specifically 97-100 and 104-110-bis) deal with data storage, criteria for deontological rules for health research, and specific provisions for health research and secondary processing in health research (described in details in the survey section on scientific research).

In **Lithuania**, the Law on Ethics of Biomedical Research was adopted in 2000. The law introduced a two-stage model of ethical evaluation of biomedical research, for the implementation of which the Lithuanian Bioethics Committee and Regional Biomedical Research Ethics Committees were selected. The Lithuanian Bioethics Committee issues permits for biomedical research and coordinates its ethical supervision. In order to implement the above-mentioned functions, a group of biomedical research experts has been formed. This group of experts is responsible for evaluating the documentation of biomedical research projects and deciding on the ethical acceptability of these researches. Both the principles of conducting clinical trials and procedural matters, requirements for investigators and research orders and their responsibilities are only comprehensive regulations and orders of both Lithuanian and international institutions for the conduct of documents and mandatory research. A study in humans can only be carried out when there is scientific and practical value to the study and the rights of the persons involved in the study are guaranteed. Even stricter protection requirements apply to certain groups of patients who, due to certain circumstances (age, medical condition, dependence on the researcher, etc.), have time violations in the research groups (e.g. children, mentally ill people, researchers' subordinates). "Involving them in clinical trials" provides even more stringent protection: studies can only be performed when they cannot be performed with other patients. No additional laws were introduced after the implementation of the GDPR.

In the **Netherlands**, consent is the first legal basis for research. Three acts are working in tandem here, being the Act on the treatment contract, the GDPR and the Dutch Act executing the GDPR. In the case of further use of patient data, the obligations from the Act on the treatment contract come first. Release of patient data outside the treatment team will need consent unless there is a legal exception. The Act allows for a limited exception in the case of research if it is impossible or not feasible to ask for consent. In that case patient data can still be released for research purposes if the research serves the common interest, the research cannot be performed without the data, sufficient safeguards have been taken to prevent re-identification and the patient did not opt out for such use. So that Act only gives an exemption to the principle of medical confidentiality in the case of research. The receiving researcher would still need a legal basis. In the case of researchers inside the same controller (such as at a large university hospital) the controller and hence the research could arguably use 5.1.b GDPR. If the data would be sent to a new controller, such as a separate research organisation, that new controller would need a legal basis of its own. If not consent in the sense of the GDPR and apart from a legal basis in article 6 GDPR, article 24 of the executing Act states that research can be performed without consent if certain conditions are met. In essence those are similar to those for releasing patient data for research without consent by the treatment team. Though not based on an official regulation, pseudonymisation has become the norm for handling personal data in research. In practice the opt-out system has been used for many research projects. This system is under discussion at the moment. Many university hospitals are considering asking explicit consent at the start of treatment or are implementing such a system. It remains to be seen whether such a system can be compatible with the requirements for consent of the GDPR without resulting in research silos and ignoring cross fertilisation of research in various related diseases areas. It is believed that the view of the EDPS in its preliminary Opinion on research of January 2020 and giving more leeway for Recital 33 than the EDPB has done in its Opinion on consent, will be helpful in this respect. In the Netherlands a Code of Conduct on health research is being prepared which is meant to give authoritative guidance on these issues. Submission to the Dutch Data Protection Authority is foreseen in late spring 2021. There is no legal obligation for approval by an ethics committee of observational research. Yet, all major hospitals and research organisations have instituted committees to vet observational research, sometimes under names as privacy committees or data access committees.

In **Malta**, Subsidiary Legislation 528.10 (processing of personal data (secondary processing)

(health sector) ("SL 528.10") permits the processing of personal data (and therefore sharing) for secondary purposes where such processing is related to:

- the processing and analysis of records kept by all entities falling within the ambit of the health sector, and the administration of the systems and services by entities, which entities are licensed to deliver any kind of service to patients or individuals, for the purpose of managing and enhancing the health service;
- the analysis of health records supplied to the Ministry for Health in accordance with licensing legislation, contractual obligations, compliance with EU regulations on public health statistics and to safeguard other public health interests, to produce the indicators required for monitoring, to ensure the quality and cost effectiveness of the health services at national level;
- the monitoring of contractual obligations, including the purposes of quality control, management information and monitoring of such services and systems, arising from the public-private partnerships and partnerships with non- governmental organisations which the Ministry for health has entered into with third parties, to ensure that the afore-mentioned partners are adhering to their contractual obligations to deliver a safe and accessible service;
- the fulfilment of the obligations related to the provision of statistical information, whether to international organisations or local clients; this may involve the linkage of existing administrative databases and disease registers;
- the compilation of evidence in medico-legal cases and in cases referred by public bodies, in the course of exercising their duties as provided by law;
- the investigation and monitoring of health threats, which typically requires the processing of health record data for the protection of public health; and
- access to health records, for the purpose of research activities.(a) the processing and analysis of records kept by all entities falling within the ambit of the health sector, and the administration of the systems and services by entities, which entities are licensed to deliver any kind of service to patients or individuals, for the purpose of managing and enhancing the health service;

In **Poland**, pursuant to the Act on Patient Rights and Patient Ombudsman, medical documentation may be submitted for research only on the basis of the patient's consent. Documentation in an anonymised form may be transferred to a scientific institution without obtaining such consent. As part of the modernisation of the act on the professions of doctor and dentist (which will come into force on 1 January 2021), the definition of a medical experiment has been extended to include research on human biological samples. On the basis of the amended regulation, each entity that wants to conduct scientific research on human biological samples must fulfil a number of obligations specific to a medical experiment, such as obtaining an opinion from a bioethical commission or insurance of the participant of the study. The regulation does not apply to research on patient data, but only applies to research on human biological samples.

In **Hungary**, scientific research is listed among the purposes of data processing under Section 4 of Act XLVII of 1997 on the Processing and Protection of Health Care Data and Related Personal Data („Medical Data Act"). The special rules for research are included in Section 21. Under para (1), anyone can have access to medical data with the permission of the head (director) or the DPO of the given healthcare provider with the aim of scientific research. The scientific publication based on those data may not contain such health data or other personal data from which the identity of the patient could be identified. In the scientific research, stored data containing personal identifying information cannot be copied. The individuals (researchers) who had access to the data, and the purpose and date of access shall be recorded, and the records must be retained for 10 years. The refusal of the research application shall be justified by the head or the DPO. The applicant may bring the case to the court. Specific legislation applies to ethics committees. As a general rule, medical research involving human subjects requires a permit from the national or regional ethics committees. This may be applicable to research using personal health data, too. No distinction is made between public or private research.

In the **UK**, under section 251 of the National Health Service Act 2006, an organisation such as a research body must confirm they have obtained an approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by another organisation

responsible for the data (the data provider) such as an NHS Trust. A CAG approval is an approval made under section 251 of the NHS Act 2006 and its current regulations, the Health Service (Control of Patient Information) Regulations 2002, which enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed without the data provider being in breach of the common law duty of confidentiality. In practice, this means that the person responsible for the information (data provider) can, if they wish, disclose the information to the data applicant e.g. research body without being in breach of the common law duty of confidentiality.

* *The Member State descriptions in this box serve as an illustration and are not exhaustive. The descriptions are based on the answers of an additional questionnaire that was responded to by a subset of countries.*

National differences - issues for researchers

Practical examples of the impact of such differences in national laws are evident in the literature. With regard to the use of data from clinical trials at a later stage for a different purpose, a particular barrier that was raised was the variable judgements of ethics committees in considering the compatibility of research applications (to reprocess data) with the original trial protocols. Individual interpretation appears to play an important role within ethics committees, leading to variable and unpredictable outcomes. Also, of relevance is concern around the reliance on data providers, and the poor standards of existing (external) data repositories which do not meet the legal / governance standards required (Cole and Towe, 2018). Another paper highlighted on ground tensions with inter-jurisdictional clinical trials with variance in national safeguards. Sponsors of clinical trials believed they were GPDR compliant but ultimately were required by the institution to undertake considerable supplementary work for one site only to fulfil additional regulatory requirements particular to the Member State (Mee et al 2020).

5.2.3. Findings - specific legislation and legal bases used for research by third-party researchers in public and non-public organisations

In addition to appropriate safeguards for secondary processing health data, researchers must also ensure processing is carried out pursuant to an Article 9(2) GDPR lawful justification. A number of options for processing are available under Article 9(2) GDPR. Some must be implemented by EU or Member State law, which should be proportionate and provide for appropriate safeguards to protect the fundamental rights and the interests of data subjects. The Articles requiring such legislation relevant to the area of health and research are Articles 9 (2) (h), (i) and (j) while Articles 9 (2) (a), (c) and (e) are available without the necessity of further law.

The different types of controllers are a determinant, along with the activity, in selecting the appropriate lawful basis. One type of researcher is the healthcare professional (or the treatment team) who originally collected the data for the purposes of treating the patient, another is the researcher who is a healthcare professional working for the same healthcare provider and hence still part of the same controller.

Research will also be conducted by third-party researchers. Here, we distinguish between a) public sector or publicly funded researchers, and b) researchers not in public sector, i.e. between researchers based in not for profit organisations and researchers based in industry or commercial research organisations. The distinction is complicated by the fact that privately funded research can also be not for profit, such as instituted by foundations. For both for profit and not for profit third-party researchers it is possible that specific legislation has been adopted that addresses the processing of health data originally collected for the purpose of providing care and may be processed by a controller outside the treatment facility.

Lawful basis

The literature shows that identifying the correct legal bases for use in the context of research is in practice difficult. A major source of uncertainty for industry is the appropriate legal basis for processing data in the absence of explicit consent, and understanding what activities reasonably fall under the various exemptions provided by the GDPR (Cole and Towe, 2018).

It has also been highlighted that there is uncertainty to which extent existing national laws apply. For example, the processing of special categories of data repeatedly references 'on the basis of Union or Member State law.' Some believe this language is ambiguous, and it is not clear what is required in terms of the EU or Member State law for providing a 'basis.' The different interpretations lead to considerable consequences for data subjects with more administrative burden (DIGITALEUROPE 2020).

It is also worth keeping in mind some processing activities may fall under different legal bases simultaneously – particularly if an extremely narrow scope is assigned to each basis. Entities have often based their processing activities on several legal bases for example processing data based on their necessity for the performance of a contract and also seeking consent. However, this interpretation contradicts the Opinion of the EDPB on consent. One should adopt one legal basis and certainly cannot jump from consent as a legal basis to another legal basis if it is found that the consent legal basis did not meet the criteria of article 7 GDPR.

Researchers in public sector organisations

The results of the expert survey reflect the difficulties expressed in the literature and indicate a myriad of lawful bases across Member States used to process health data for research across both public and private sector. Responses for public-sector processing show that eleven Member States have not introduced legislation specifying which lawful basis should be utilised for such processing (see table 5.2).

Although highly advanced in its approach to facilitating access to data for research through a data access permit system (Findata), it is worth noting that Finland's Act on the Secondary Use of Health and Social Data does not stipulate the legal basis that should be used for further processing in public sector research. Ireland, in the Health Research Regulations 2018, takes the same approach as Finland leaving the choice of lawful basis open to controllers but regulating the safeguards required to conduct research in both the public and private sector in the context of the provisions set out in the Data Protection Act 2018.

Responses from Member States indicate that nine utilise Article 9(2)(i) and fourteen have regulated using the Article 9(2)(j) research exemption. It is important to note that in many countries several lawful bases may apply (see Table 5.2 and Table A1.34 in Annex 1).

Table 5.2 Legal base in Article 9(2) relied upon when data, originally collected for direct care, are used for research by third-party public-sector researchers.

Legal basis for processing data for research by third-party public sector researchers	Total MS	
Explicit Consent (Article 9(2)(a))	6	EE, FI, LV, IE, MT, AT
Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised	3	BE, DE, EE
Broad consent as defined in national legislation, or in accordance with Recital 33	3	DE*, FI, AT
Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask for consent) when consent may be waived	4	BE, DE, EE, NL
Article 9(2)(i) public interest in the field of public health	9	BE, DE, EE, FI, FR, HR, LV, MT, IE
Article 9(2)(j) research purposes	14	BE, DK, DE, EE, FI, FR, HR, IE, IT, LV, LU, HU, MT, AT, [UK]
Other	1	FI**
No specific legislation	12	BG, CY, CZ, ES, EL, LT, PL, PT, RO, SI, SK, SE

* *In the case of Germany, there is no mention of broad consent in legislation in the sense of legal acts but this should become administrative practice as recently confirmed by a resolution of all supervisory authorities.*

** *in the case of Finland the Act on the Secondary Use of Health and Social Data does not stipulate the legal basis that should be used for further processing in public sector research.*

Researchers in non-public organisations

The responses relating to the lawful basis for third party researchers not in the public sector again are variable. Thirteen Member States have not introduced legislation defining lawful basis for non-public sector researchers, seven rely on Article 9(2)(a) consent, three have the option of broad consent, six include Article 9(2)(i) and thirteen utilise Article 9(2)(j). Again, it is important to note some Member States allow for several lawful bases (see Table 5.3 and Table A1.34 in Annex 1).

Table 5.3 Legal base in Article 9(2) relied upon when data, originally collected for direct care, are used for research by third-party non-public-sector researchers.

Legal basis for processing data for research by third party researchers not in the public sector	Total MS	
Explicit Consent (Article 9(2)(a))	7	DK, EE, FI, LV, MT, IE, AT
Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised	3	BE, DE, EE
Broad consent as defined in national legislation, or in accordance with Recital 33	3	DE*, FI, AT
Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask for consent) when consent may be waived.	4	BE, DE, EE, NL
Article 9(2)(i) public interest in the field of public health	6	BE, DE, FI, FR, LV, MT, [UK]
Article 9(2)(j) research purposes	13	BE, DK, DE, EE, FI, FR, IE, IT, LV, LU, HU, MT, AT, [UK]
Other	1	FI**
No specific legislation	13	BG, CY, CZ, ES, EL, HR, LT, PL, PT, RO, SI, SK, SE

* *In the case of Germany, there is no mentioning of broad consent in legislation in the sense of legal acts but this should become administrative practice as recently confirmed by a resolution of all supervisory authorities.*

** *in the case of Finland the Act on the Secondary Use of Health and Social Data does not stipulate the legal basis that should be used for further processing in public sector research.*

The majority of respondents to the survey indicated that national legislation did not differentiate between for profit researchers and not for profit researchers. By way of example, France has a common legal regime applying to public and private organisations seeking to process personal data for research purposes. Nevertheless, the research purpose at stake will trigger different procedures and examinations depending on the pursuit of a public interest purpose. This translates a particular caution regarding private, for profit, personal data processing purposes and to the scrutiny of public interest justifying sensitive data processing, but there is no explicit exclusion of any special categories of data controllers or processors (see also Box 5.7).

Box 5.7 Some examples: What type of data is available for researchers*

Researchers may use different sources for obtaining data. Data may be stored by private companies, in anonymised databases (set up by private organisations or professional associations) or data can be collected in a clinical trial, done by private companies. In this Box we describe whether researchers can have access to these data; whether specific conditions have been set out; and what are the legal bases for these situations, based on the answers to the additional survey for country correspondents.

Data held by private companies

From the fourteen countries that provided information, four indicated that researchers cannot access data from private companies (Bulgaria. Croatia, Italy, Sweden).

Lithuania explained that all types of researcher may have access to these data. However, if research falls under the biomedical research category researchers need to acquire approval for the study pursuant to the Law on Ethics of Biomedical Research. Private companies need to grant consent to access such data.

Poland and **Greece** indicate that there are no specific regulations in this regard. It depends on the regulations adopted by a given entity and the terms of the data transfer agreement.

In **Slovakia**, access would be subject to the personal data protection legislation and would require consent of the data subject in most cases. The private company would most likely require a special contract to be executed by the researcher in such case. **Ireland**, **Romania, Malta**, **Sweden and UK** explain that all types of researchers may have access. **Ireland** adds that this depends completely on access being granted by the private company and appropriate REC approval being in place. There is no legislation obligating access. **Sweden** adds that there is no nationally regulated obligation to share data for research. In the **UK**, researchers can always apply for data access held by private companies. It is up to the private company as to whether they are willing to grant access to researchers, and the conditions under which such access may be granted. But there is no legal provision for this. In the **Netherlands**, private companies are not legally obligated to grant researchers access, but they are allowed to do so if the data subject has consented or if an exemption to the consent principle would apply but private companies have been very hesitative to use the latter.

Data in anonymised databases

From the eleven countries that provided information, only two (Lithuania and Sweden) indicated that it was not possible for researchers to access anonymised databases of patient information set up by private organisations or professional associations (e.g. registries of specific associations). However, there are currently law proposals on this in the Lithuanian Parliament, but these are at the date of preparing this report not yet formally adopted. Examples of countries were access is possible are Bulgaria, Denmark, Greece, Ireland, Italy, The Netherlands, Poland, Slovakia, and the UK. Generally, these countries do not have specific legislation for this situation.

In **Bulgaria**, the access applies to publicly funded organisations. The legal basis is the National Health Act, art. 28 – Anonymised information for the need of the Public health and statistics.

Denmark indicates that some medical registries have been set up by researcher or medical societies and they can be accessed as other research data under consideration of pseudonymisation and data protection as well as the confines of the informed consent. The

International Chromosomal breakpoint consortium is one example.

In Ireland, all types of researchers can have access. The legal basis depends on the circumstances. Relevant questions here relate to whether it is a public or private researcher, there is consent from the data subject, and there is a public interest.

In **Italy**, if a private organisation set up a database with the purpose of sharing anonymised patients data, these can be accessed by third party researchers. It largely depends on the specific conditions set for accessing the database.

Slovakia adds that no special conditions would apply in such situation with the exception of the personal data protection legislation, consent of the data subject (if applicable to such anonymised database) and the licensing terms of the database.

In **Poland**, access is only possible when the entity that creates the database makes the data available.

Access to clinical trial data

Can researchers access information related to clinical trials done by private companies? Four countries answered yes (Denmark, Ireland, the Netherlands, and the UK); five countries answered no (Italy, Poland, Romania, Slovakia, and Sweden). In general, these countries do not have specific legislation for this situation.

Denmark explains that this is only possible when the company wants to share the data. In **Ireland**, a comparable situation exists. There is no obligation in law requiring private companies to give access to clinical trial data, it is up to the company. In the **Netherlands**, private companies are not legally obligated to grant researchers access, but they are allowed and would be ethically compelled to do so if the data subject has consented. A Data transfer agreement will be drafted for this access. **Slovakia** explains that there is no legislation in place granting such access. This does not exclude possible provision of such data under contract by and between the private company and the researcher. In the **UK**, there is no specific legal basis. A data access application can be made, and the researchers would need to state their compliance with relevant data protection law, i.e. GDPR/Data Protection Act 2018.

* *The Member State descriptions in this box serve as an illustration and are not exhaustive. The descriptions are based on the answers of an additional questionnaire that was responded to by a subset of countries.*

Reflection

While the GDPR harmonises cross-European data protection law to facilitate the free flow of data across Member States, it is evident from the mapping of Member States' legislation and feedback from national experts, that there are divergences in the application of the GDPR in the context of health research. The results of the study show Member States are extensively utilising the margin of manoeuvre afforded in the GDPR. It is evident there is a variance of safeguards and lawful basis leading to confusion and technical difficulty when conducting inter-jurisdictional research. The literature review highlighted particular difficulties with interpretation of the meaning of terms namely; the definition of public or private researcher and what happens when there is a hybrid anonymisation and pseudonymisation definition. Aside from these problems examined by this study it is important to note the interplay of data protection with ethical requirements for research. The literature points to the problem that differences in Member State ethical requirements for health related research could hamper EU collaboration. Ethical vetting is done by a Research Ethics Committee (REC, though this vetting function may go under different names for observational research, such as privacy committees) which may be instituted at the level of the research organisation or at the regional or national level. In addition, some countries require additional approval by the National Data Protection Authority. Another example is how national RECs organise their approval: What kind of documents need to be submitted to RECs? This can

vary not only between Member States but also from one institutional REC to another (Timmers et al 2018).

5.2.4. Specific legislation and legal bases used for research on genetic data

The field of genomics is rapidly advancing, with high hopes of revolutionising health provision, among others by means of better and personalised diagnostics, medicines, therapies and interventions. For example, the "1+ Million Genomes" initiative aims to have at least 1 million sequenced genomes available in the EU by 2022, and its declaration, part of the EU's agenda for the Digital Transformation of Health and Care, is signed by 21 Member States and Norway.[17]

Genetic data and genomic data

It is firstly important to understand the difference between genomics and genetics. The World Health Organisation defines genetics as the study of heredity and genomics is defined as the study of genes and their functions, and related techniques (WHO 2002; WHA 2004). The main difference between genomics and genetics is that genetics scrutinises the functioning and composition of the single gene whereas genomics addresses all genes and their inter-relationship in order to identify their combined influence on the growth and development of the organism (WHO 2002, WHA 2004).

The GDPR refers to genetic data but not genomic data. It provides a definition of genetic data at Article 4(13) and again refers to genetic data as a special category of personal data at Article 9. However, there is a certain level of uncertainty and disagreement as to whether genomic data are also covered by the definition of genetic data in the GDPR. The PHG Foundation, in a report issued in 2020, highlights the uncertainty about which data, resulting from what forms of analysis, fall within the GDPR definition. Noting this challenge, the report suggests that the genomics community should be proactive in developing appropriate standards for de-identification of genomic data through a code of conduct or certification scheme setting out best practice for specific contexts and forms of data. This could help build consensus and achieve harmonisation of national and international approaches under the GDPR given the potential that such a code or certification scheme may be formally recognised under the GDPR

When it comes to genetic data, the Oviedo Convention must also be observed. It entered into force in 1999, and in combination with its additional protocol concerning biomedical research, aims to provide a legally binding instrument to protect human rights with regards to biomedical data, including genetics and transplantation of organ and tissues. However, the convention only sets a minimum threshold of due notification, and does not concern research making secondary use of biosamples and genetic data (Pormeister 2018). In addition, the additional protocol concerning research was only ratified by six EU Member States (BG, CZ, HU, PT, SK, SV, of which CZ recently in May 2020) and a total of 12 countries[18]. As a result, and in line with Article 1 of the Oviedo Convention, room is left for national laws to provide regulation. With the introduction of the GDPR this has not fundamentally changed.

[17] The full list of countries is Austria, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Portugal, Slovenia, Spain, Sweden and the UK.

[18] See the official website of the CoE for the 'Chart of signatures and ratifications of Treaty 195', https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/195/signatures?p_auth=MXKewYR9 (accessed July 19, 2020).

Findings - Member states' legislation regarding research with genetic data

While the GDPR defines genetic data[19], it does not provide a harmonised regulatory context as the rules governing the research; use of genetic data will in a large part be subject to national interpretation and already existing laws. The GDPR also does not govern as such the biological samples from which genetic and genomic data may potentially be derived. In this respect, Article 9(4) GDPR allows Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, resulting in a situation where a few countries, such as France, Finland and Italy have specific provisions governing genetic research, whereas others do not.

Country correspondents were asked if legislation regarding genetic data had been introduced in their Member State, thirteen reported that in their Member State such legislation had not been adopted (Table 5.4). The survey also asked if the law differentiates between not for profit researchers and for profit researchers, but none of the 14 Member States reported as having legislation in place indicated to make such a distinction. The survey further examined if such legislation chose different legal bases for processing genetic data than other health-related data - in this case 8 Member States indicated the legal grounds to process data differed for genetic research to other research, while 7 did not.

Table 5.4 Member States' legislation regarding research with genetic data

Legislation on genetic data	Total MS	Member States
No specific legislation has been adopted for research with genetic data	13	BE, CZ, DE, FI, EL, CY, LT, LU, MT, PL, RO, SI, SK, [UK]
Specific legislation has been adopted for research with genetic data	14	AT, BG, DK, EE, IE, ES, FR, HR, IT, LV, HU, NL, PT, SE
If yes, this legislation does not differ from the legal grounds to process other data for research	7	EE, IE, HR, MT, PL, SE, SI
If yes, this legislation differs from the legal grounds to process other data for research	8	AT, BG, ES, FR, HU, IT, LV, NL

In Member States where specific legislation for genetic research has been introduced, the legislation varies in its requirements. This ranges from an obligation to obtain explicit consent in Hungary, while in Spain under Law 14/2007 on Biomedical Research there is a legal requirement to notify subjects about the possibility of finding unexpected results or results that may affect relatives. There is also an obligation under Spanish law to return results relevant to health and to provide genetic counselling; the expert's response indicated uncertainty however as to the status of this law following the introduction of new data protection law. The Italian feedback indicated that pursuant to art. 2-septies of the Data Protection Code, the Italian DPA must adopt provisions outlining safeguards measures with regard to the processing of genetic, biometric, and health-related data however, these safeguards measures have yet to be issued by the DPA.

Austrian legislation was reported as specifying that genetic analyses on human beings for scientific purposes can only be carried out on de-identified probes and linkage can only be performed by institutions with consent from the proband in line with Article 4(11) GDPR (see Table 5.4 and Box 5.8).

[19] Article 4(13) of the GDPR defines genetic data in a broad manner, meaning 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question'.

Box 5.8 Austria - Austrian Legislation Relating To Genetic Data

Two pieces of sector-specific legislation provide separate or additional provisions for research with genetic data.

Article 66 of the Federal Gene Technology Act (Gentechnikgesetz) specifies that, in addition to relevant provisions in FOG (Art 2d(1, 3-8), 2f(1)(6), 2f(3, 4, 6, 7), 2i(1, 2, 2j), 2j and 2k are quoted), genetic analyses on human beings for scientific purposes can only be carried out on de-identified probes. Non-genetic health data that are to be linked to the genetic data of a person likewise have to be de-identified. Data linkage may only be performed by institutions that obtained informed consent from the proband according to Art. 4(11) GDPR. Results of genetic analyses can only be published if appropriate measures are in place to avoid re-identification.

Art 19(4) of the Federal Act on Reproductive Medicine (Fortpflanzungsmedizinigesetz, FMedG) specifies that processing of data related to reproductive medicine interventions for scientific, historic or statistical purposes has to be limited to pseudonymised data if this allows the research purposes to be met. If identified personal data is necessary for the research purposes to be met, the rights of the data subject according to Art. 15, 16, 18 and 21 GDPR can be excluded in so far as these rights would render impossible or seriously impair the realisation of the specific purposes.

Genetic research - rapidly developing

In line with the European Union's "1+ Million Genomes" initiative, there is a growing body of international genomics projects, many of them making use of cloud services, including the Pan-Cancer Analysis of Whole Genomes (PCAWG) Project, The Human Cell Atlas, and the European Open Science Cloud.[20] Legal experts involved in the PCAWG Project have pointed to the challenges that such cloud services bring to the protection of participants' data, and they therefore call for an international code of conduct that can help researcher establish clear ethical and legal guidelines on how to use genomic data, and cloud services in particular (Phillips et al, 2020; see also chapter 8). The Dutch so called ELSI service desk will soon together with the MLC Foundation publish a report on the ethical challenges of using private clouds for genetic research. One of the main findings is that though these cloud providers can offer additional security and scalable pipelines for research without excessive costs it is often difficult to maintain a clear separation of roles between controller and processor considering the market power and other interests of the few large private providers.

Concerns have also been raised around the advancements in DNA sequencing and profiling technologies and the ability of corporations to track and categorize individuals is growing, which raises the risk of commodification practices of consumers' sensitive health identities. These sophisticated processing technologies are controlled by just a few big players (Schneider 2019). While others have raised questions around the use of consent in particular the specificity of consent for genetic and genomic research when relying on Article 9(2)(a) GDPR and interpreting its interplay with scope of broad consent in Recital 33 (Hallinan 2020). Hallinan notes that broad consent is used in most studies and claims that this could inform the European standard just as it is the ethical standard in other jurisdictions.

[20] As example, the Pan-Cancer Analysis of Whole Genomes (PCAWG) Project performed whole genome sequencing and integrative analysis on over 2,600 primary cancers and did so, making use of the Cancer Genome Collaboratory, a cloud service built for the genomic research community, with data being processed in the clouds academic institutions in Germany, the United Kingdom, the United States, Canada, Spain, Japan and South Korea, in addition to some commercial clouds being used (Phillips et al, 2020).

Reflection

The results of the expert surveys show once again a variance across Member States with regard to genetic research. Where legislation has been adopted there are differences in the safeguards and lawful bases applied. The findings reflect concerns expressed in the literature, for example, Shabani and Borry (2018) note that increasing cross-border data-sharing underlines the importance of the harmonisation of legal frameworks concerning data protection and have concerns that the GDPR was leaving room for varying interpretations across Member States. They note in particular concerns around the application of safeguards and Member States setting further conditions for processing genetic data.

The unique scope and potential impact on data subjects of genetic/genomic research, raises questions as to whether it should be viewed as a special category of health research in itself. Some have observed that genomic research may be seen as a unique construct (Karsten et al 2011). Hewitt notes no other form of health research aims at the systematic analysis of genome function, expression and genome-environment interaction; no other form of health research promises to provide the stratification of populations needed for the development of precision medicine systems; and no other form of health research supports the development of genetically targeted medical interventions (Hewitt 2011).

5.3. Consent

The concept of consent in the Data Protective Directive (Directive 95/46/EC) has evolved and GDPR sets out stricter requirements for obtaining valid consent from data subjects. In practice, GDPR raises the bar with regards to implementing consent with validity relying on cumulative criteria set out in Article 4 (11), Article 7 and recitals 32, 33, 42, and 43 of GDPR being met. Numerous European opinions[21] have stated that GDPR consent will not always be the appropriate legal basis for processing personal data in health research, particularly in the context of clinical trials and in view of the existence of a power imbalance in healthcare settings. The Health Research Authority in the UK advises against the use of GDPR consent as a legal basis for processing for health and social care research primarily due to power imbalance, but notes informed consent is still required to fulfil obligations under the common law duty of confidentiality. France similarly has made it clear that they require informed consent but not the consent defined in the GDPR, rather as a safeguard. In both of these examples consent is required but not in a GDPR sense, rather as a national safeguard for the participation of individuals in research. Ireland, on the other hand, has applied a blanket requirement of explicit consent under GDPR as a requirement for both primary and secondary research. Stakeholders report that this has been a burdensome requirement having considerable impact on the conduct of research. Particular problems have arisen around the need to re-consent, the conduct of retrospective chart review, capacity, pre-screening and the

[21] Article 29 working party guidelines on consent under regulation 2016/679. European Commission. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051;
European Data Protection Board (2019a). Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)(art. 70.1.b));
European Commission https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.; European Commission (2019a). Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation. European Commission.
https://ec.europa.eu/health/ sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf;
European Data Protection Supervisor. A preliminary opinion on data protection and scientific research. European Commission. https://edps.europa.eu/sites/edp/files/publication/20-01-06_ opinion_research_en.pdf.

use of bio-bank/archival material. Another concern raised by this approach is the creation of bias (Kirwan et al 2020).

The literature identifies many circumstances in which consent would not be the most appropriate lawful basis. Dove stressed that consent is only one of several legal bases for processing personal data. In other words, researchers who seek to collect and use data from patients and participants may not need to rely on consent as their legal basis; and often in the research context, consent is not the most appropriate legal basis, particularly in large-scale epidemiological studies or genetic studies (Dove 2018). Chico raised the concern that reliance on consent might devalue some scientific research (Chico 2018).

Recent opinion from the European Data Protection Supervisor (EDPS) issued in January, 2020 highlighted the difference between Member State national requirements for informed consent to research and consent as specified in GDPR. It contended informed consent could serve as an 'appropriate safeguard' although stated that under what conditions such informed consent might be deemed an appropriate safeguard is still unclear (European Data Protection Supervisor 2020).

From the survey and workshops, it is clear that understanding and application of consent can vary significantly across Member States. Countries are not always talking about the same type of consent when discussing the topic. Some refer to informed consent based in national law while others refer to explicit consent in the GDPR. It is clear this is an area that needs greater discussion and clarification.

Box 5.9 Some examples: Can stakeholders, other than the patient, block the release of patients' data for research, despite patient's consent that these data can be used?*

Blocking by healthcare providers

When a patient gave consent to share data for research, healthcare providers will be asked to provide the patient's data. In this box, the option for healthcare providers to block this data sharing is explored. Fourteen countries provided information on this issue. Ten countries indicated that this was not possible (Bulgaria, Croatia, Greece, Lithuania, Malta, the Netherlands, Poland, Slovakia, Romania, and the UK). In the countries that answer positively, in general, data can be blocked if no formal approval is obtained:

In **Ireland**, in the event the researcher does not gain Research Ethics Approval a healthcare provider can block release even where a patient has consented that the data can be used for research.

In **Italy**, a healthcare provider is entitled to make agreements with third party researchers in order to transfer patients' data for which consent has been provided. As an example: a patient provides consent to healthcare provider A for the transfer of personal data to third party researchers for research purpose. This, however, does not mean that data can be "automatically" transferred. Healthcare provider A will make agreements (typically, a data transfer agreement) for transferring the data. However, Healthcare provider A is not obliged to do so.

In **Hungary**, under Section 21 of the Medical Data Act, access to medical data for research purposes requires the permission of the head (director) or the DPO of the given healthcare provider. Refusal of the request shall be justified by the head or the DPO. The applicant may bring the case to the court.

In **Sweden**, the healthcare provider may only release patients' data after an approval from the Ethical Review Authority. The patients' consent doesn't change this. If it's a public care provider, the organisation is obliged to make data accessible to anyone who asks for it, if no regulation on secrecy apply (if researchers ask for data after an approval from the Ethical Review Authority, the data should accordingly be made available). This follows from the Public Access to Information and Secrecy Act. If it's a private care provider, there is no similar

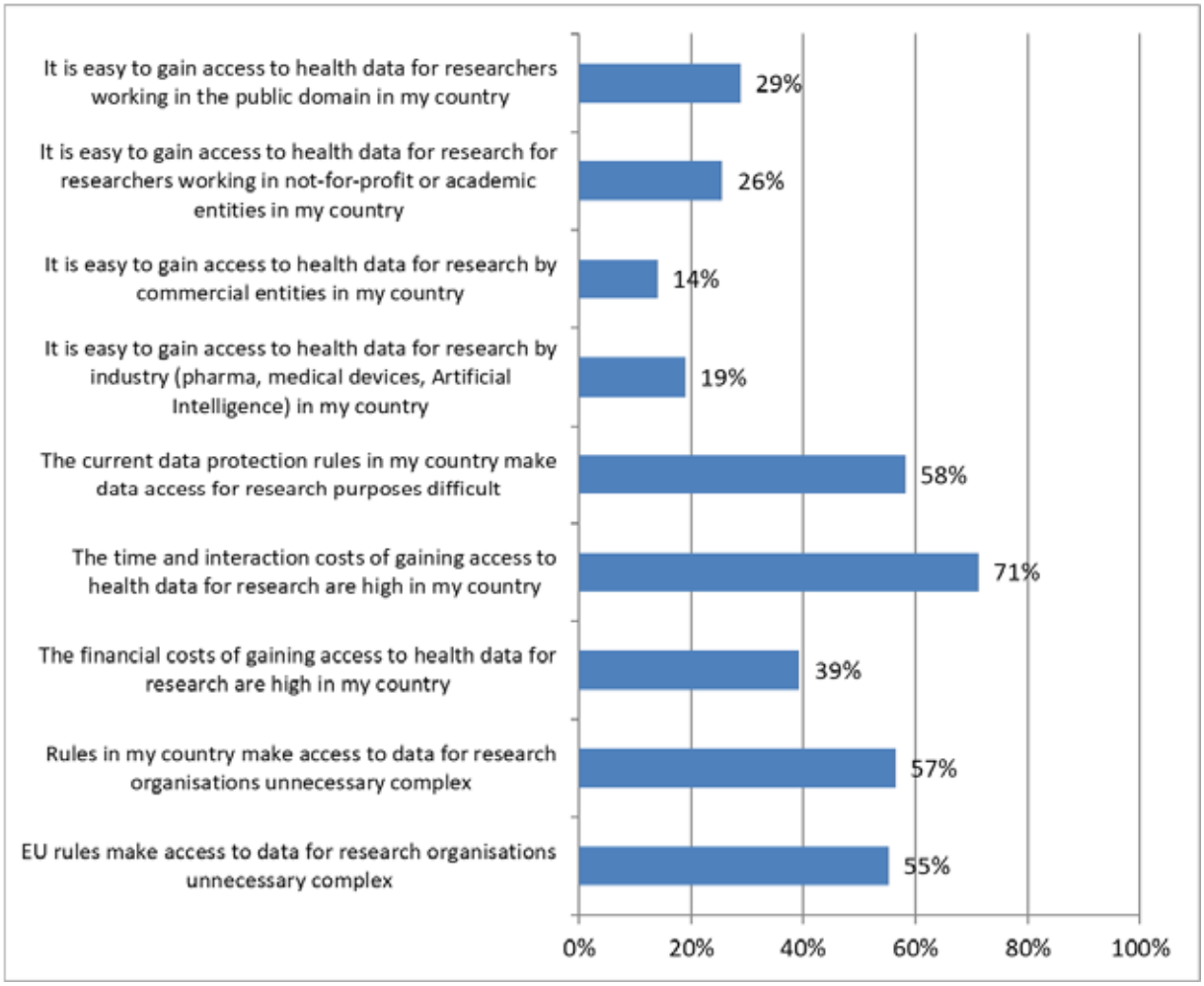
obligation in the national regulation to make data accessible. In accordance, a private care provider may transfer data for research after an approval from the Ethical Review Authority, but is not obliged to do so. However, in practice it appears as very unlikely that a private care provider would block the data, particularly if the patient consented.

* *The Member State descriptions in this box serve as an illustration and are not exhaustive. The descriptions are based on the answers of an additional questionnaire that was responded to by a subset of countries.*

5.4. Stakeholder views concerning processing personal data for research purposes

The results of the stakeholder study indicate very poor levels of access to data for public researchers across member states. Commercial entities found it most difficult with only 14% responding that is was easy to access data, while 71% felt the cost and time needed to gain access to data was high. Interestingly more stakeholders felt national rules made access to data more complex than EU rules (see Figure 5.1).

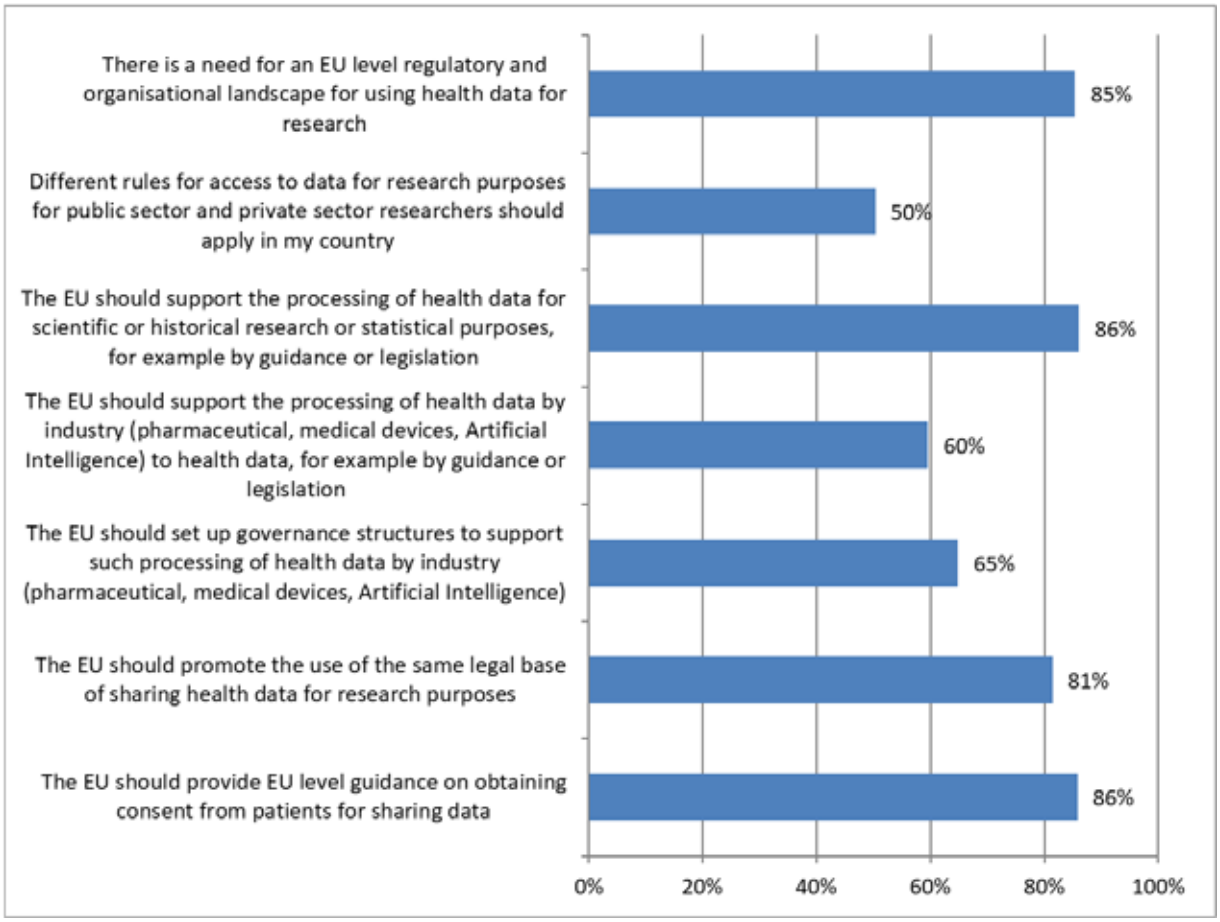
Figure 5.1 Share of stakeholders agreeing with the following statements, all related to the way in which data sharing for research purposes is possible



In relation to the need for an EU regulatory and organisational landscape for using health data, 85% of stakeholders felt it was required. Only half felt there should be different rules for public and private sector research, and an overwhelming 86% thought that the EU should support the processing of health data for research by guidance or legislation. Equally high at 86% were those seeking guidance on consent for data sharing. A large

share (81%) also supported the promotion of the same lawful basis for sharing data for research (see Figure 5.2).

Figure 5.2 Share of stakeholders agreeing with the following statements, all related to whether data sharing for research purposes should be improved



In conclusion, researchers currently find access to data difficult with cost, time and national rules cited as the main factors. Stakeholders overwhelmingly support the introduction of EU guidance or legislation to support researchers.

5.5. Concluding remarks

The issues discussed above focus on how differences between Member States in the implementation of GDPR affect data accessibility for researchers. The main message to emerge from the analysis is that there are different rules and regulations governing access to health data both within and between Member States, which impact researchers both in the context of in-country and cross-border research. They make it hard for researchers to understand how the rules governing the processing of health data apply in their intended research, this issue is more evident for research using genetic data, but is seen by researchers working in most areas. These differences have an effect on the accessibility of health data in themselves, and they also relate to a number of other factors that affect the availability and accessibility of health data, including the respect of data subjects' rights. As stated in the European Patients' Forum response to the Public Consultation on the European Strategy on Data, it is essential that individual rights which apply to patients - access to one's personal data, exercising control of their data, transparent information about processing, and the right to be forgotten or to erase data - are effectively implemented, with patient friendly information and transparent processes.

The responses of the expert correspondents and stakeholders indicate a high level of interest in further EU level action to create a more level, and above all more understandable, playing field for research using health-related data. As discussed above 85% of the stakeholder respondents saw a need for EU level legislation, with over 80% supporting action to address the role of consent and action to drive more common approaches to the legal bases used to legitimate data re-use for research.

6. DATA SUBJECTS' RIGHTS

6.1. Introduction

The GDPR grants several rights to the data subjects, which may be summarised into four broad categories as set out in box 6.1 below:

Box 6.1 Data Subjects' Rights

- **Information** and **transparency** (Articles 12,13,14): The data subject has the right to be clearly informed why the data is needed, how it will be used and to whom it will be accessible. This includes giving contact details of the data controller, and where applicable the data protection officer, to respond to a data subject's questions in a timely manner. The data subject must be informed if the processing is carried out based on consent and of their right to withdraw consent in such case. Where the legitimation for using data is based in the data controller's legitimate interest (Article 6(1)(f)), such legitimate interests must be clearly explained. The data subject must also know for how long data will be stored, and be informed of the existence of data subjects' rights as well as the right to lodge a complaint with a supervisory authority.
- **Access** (Article 15) **Rectification** (Article 16) **Erasure** (Article 17) or **Restriction** (Article 18) and **Objection** (Article 21): Article 15 provides that the data controller must provide access in the form of copies of the personal data being processed, and where data are processed electronically such copies should be electronic. The right of correction means the data controller must correct any inaccuracy the data subject identifies as soon as possible. The data subject has the right to restrict processing while correction takes place. Erasure, also known as 'the right to be forgotten' is available in specific cases, for example if the data are no longer necessary for the purposes for which they were collected or when the data subject withdraws consent. However, Article 17(3)(c) states the right shall not apply when data are processed for healthcare provision (Article 9(2)(h)) or public health purposes (Article 9(2)(i)), while 17(3)(d) extends the exemption to data processed for scientific research purposes in accordance with Article 89(1). Article 21 provides the right to object to processing carried out on the basis of public interest (6(1)(e)) or legitimate interest (6(1)(f)), on grounds relating to his or her particular situation. However, such right is excluded in the context of scientific research when the processing is necessary for the performance of a task carried out for reasons of public interest.
- **Data Portability** (Article 20): The data subject has the right to receive a portable copy of any data concerning him or her that he or she provided to a data controller. This should be provided in a common machine-readable format and must allow the data subject to transfer the data to another data controller. This right is however restricted to data which has been processed on the basis of consent or a contract and which is processed by automated means.
- **Automated decision making and profiling** (Article 22): With respect to automated decision making, a data subject may object to any automated processing where such processing produces legal effects or similarly affects him or her, except where processing is based on the data subject's explicit consent, is necessary for entering into or the performance of a contract, or when the processing is authorised by Union or Member State law which lays down suitable safeguards. Automated processing that produces a legal or other significant effect on the data subject may not be undertaken with **sensitive data** as defined in Article 9(1) unless the data subject has provided explicit consent or the processing is necessary for reasons of substantial public interest on the basis of EU or Member States law

In accordance with Article 23 GDPR all the rights outlined above may be limited by Union or Member State legislation, so long as such restrictions respect fundamental rights and freedoms and are necessary and proportionate in a democratic society. Following article 89(2) GDPR some of those rights can also be limited in the context of scientific research while article 17(3)(d) provides a directly applicable research exemption to the right to be forgotten if the

conditions of that clause are met.

Additionally, it should be mentioned that, as pseudonymisation is the norm in the data chain for research, article 11 GDPR will apply to most of the data arriving at the research organisation. That article states in sum that the controller is not obliged to comply with the obligations of articles 15-20 if it does not have access to direct identifiers of the data subject unless the data subject provided additional information by which the controller could uniquely identify the data subject.

The rights as described in box 6.1 are general rights that apply to all data subjects and all types of data. However, when these rights are applied to health-related data and in the healthcare setting they must be interpreted in the context of healthcare, where a number of other legal requirements with respect to data will exist at national level. Most importantly this will include regulations that require health-related data to be collected and processed in a particular way, often including minimum retention periods. In most countries there will also be legal provision to facilitate accessing or processing data in an emergency situation where usual rules of providing information to the data subject cannot be adhered to, as well as situations where normal rules of access to data by the patient may be overruled in the interests of protecting the patient or others. Such exceptions are much less common than they once were, overriding of patients' rights now almost always requires careful justification and documentation, but nevertheless, in the healthcare setting the rights as set out in box 6.1 cannot always be exercised as a matter of absolute right. The GPDR itself foresees this, providing in Article 23 (1) that Union or Member State law may be adopted that limits the rights in Articles 12-22 in certain circumstances, including the interests of public health or the protection of the data subject or the rights and freedoms of others (Article 23(1)(e and i)). However, such restrictions must be laid down in Union or Member State legislation which respects the fundamental rights and freedoms of individuals and must be necessary and proportionate to the public or individual interests that are being safeguarded. Such rights may also be restricted in the context of data used for research purposes, if this is based on national law implementing Article 89(2) GDPR and its fulfilling conditions.

6.2. Survey finding on patients' and data subjects' rights with respect to health-related data

Both surveys (national experts and stakeholders) included questions looking at how the rights as set out in box 6.1 are applied at national level. In this chapter we begin by looking at the duty of transparency and the rights of the data subject to be informed about why and how data are processed, looking at this particularly in the context of re-use of data for research. We then consider the right of access, and the associated rights of rectification and erasure, before discussing the right of portability and considering the practical issues associated with making that right a reality for patients. Finally, the chapter considers the responses of stakeholders to questions on how they experience the exercise of rights in the area of health and how this experience might be improved. The surveys did not include questions about automated decision making as addressed in Article 22 GDPR. As with other parts of this report, the answers provided by both Member State level correspondents and the stakeholders must be considered within the context of the healthcare systems in which they operate.

6.2.1. Transparency and information

As set out in box 6.1 above, the GDPR requires that the data subject is provided with transparent information about the way in which his or her data are to be processed. Article 12 GDPR requires that transparent information about the processing must be provided in a clear, accessible and intelligible manner, meaning that issues of intellectual capacity to understand as well as physical aspects of accessibility, such as font size in written information, must be taken into account. Article 13 sets out in detail the type of information which must be provided when data are collected directly from the data subject, while Article 14 describes how the data subject is to be informed when data were collected from another source.

Transparency and research

Recognising that in the research context it is not always possible to provide information, the GDPR provides in article 14(5)(b) for some exceptions when data are processed for scientific or historical research purposes or statistical purposes as long as Article 89(1) safeguards have been put in place. Therefore, when a research organisation receives data from a party such as a health care provider, the controller may be exempted from informing the data subject about the use of the data where the provision of such information proves impossible or would require a disproportionate effort or insofar as doing so is likely to render impossible or seriously impair the objectives of that processing. In such cases, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. This might therefore include general publication about the use of data on the organisation's website or other public information channel.

Furthermore, where the data controller can demonstrate that it is not in a position to identify the data subject, in particular because the purpose of the processing does not require or no longer requires the identification of the data subject, then Article 11 applies and the rights and duties outlined in box 6.1 will not apply. Where possible, the data controller shall inform the data subject accordingly. Article 11 GDPR states that when the data subject is not identifiable, the controller shall not be obliged to acquire additional data to comply with the data subjects rights of the GDPR, unless the data subject provides additional information enabling his or her identification.

Keen to further understand the impact of the Articles described above on the use of data for research, the survey completed by the country correspondents asked two questions specifically related to data subjects' rights in the context of health data used in research (see Table 6.1 for Member States that adopted further legislation).

The first, reflected in table 6.1 below asked if any national level legislation had been adopted that further clarifies the rules on transparency of data processing in research projects. Seventeen Member States indicated that no additional legislation had been adopted. The correspondents for DK, FR and EL explain the role of ethics committees and special provisions in national law that make use of the exception provided for in Article 14(5)(b) GDPR.

Table 6.1 Member States that adopted legislation that further clarifies or details the requirements set out in the GDPR about the transparency and accountability of researchers or research projects (including the rights in Articles 13 and 14)

Adopted legislation that further clarifies or details the GDPR for research purposes	Total MS	
Yes	10	DK, DE, EE, EL, FR, IT, LV, HU, AT, SI, [UK]
No	17	BE, BG, CZ, IE, ES, HR, CY, LT, LU, MT, NL, PL, PT, RO, SK, FI, SE

A further question asked if Member States had adopted any restrictions to data subjects' rights where data are used in research as provided for in Article 89(2) GDPR. Here it is interesting to note that all but six Member States had adopted such legislation at national level, as shown in table 6.2. Typical examples of such limitations are that rights to rectification or erasure are limited when to rectify or erase would compromise research already underway and when removal of data would be extremely difficult where it is already used within a study. For Belgium it was noted that, unless a Code of Conduct has been adopted in accordance with Article 40 GDPR to address the issue, the data protection officer of the research organisation will be required to provide explanations to the Data Protection Agency as to how the maintenance of data subject rights would impede research and why an exemption should apply. Of those correspondents who replied in detail to this question with examples, most gave examples related to access and rectification rights rather than information rights, these examples are further discussed below.

Table 6.2 Did Member States implement the exceptions to the rights of the data subject for research following article 89(2)?

Adopted legislation that further clarifies or details the GDPR for research purposes	Total MS	
Yes	14	BE, CZ, DK, DE, EE, IE, EL, HR, LV, LU, MT, AT, RO, FI
Yes, partially	5	ES, FR, NL, SI, SE, [UK]
No	6	BG, IT, LT, HU, PL, SK
Not sure	2	CY, PT

6.2.2. Access, rectification and erasure

The rights set out in Articles 15, 16 and 17 related to access, rectification or erasure of personal data respectively, are particularly complex in the case of health-related data and must be understood in the context of healthcare provision and research. Although the GDPR confers these rights as a matter of general principle, in the healthcare setting they have to be understood within a wider framework because a healthcare record is not only a record of data concerning a patient, it is also a record of the professional interventions as well as the reflections and opinions of the healthcare professionals who interact with the patient. In the Netherlands the medical file is the primary basis for assessing the performance of the professional in the context of disciplinary or tort proceedings.

The obligation to record all relevant facts concerning the patient is laid down in law (see also chapter 3), the content of the file is described in professional guidelines. If the medical file is sloppy, the professional will usually not be able to prove his or her case that the diagnosis or treatment was according to the professional standards. The patient cannot request the file to be deleted during the proceedings. If he or she would have done so earlier, the (disciplinary) court would dismiss the case as the patient would have made it impossible for the professional to defend him- or herself. The professional may share the medical file with his or legal advisor after a complaint without breaching medical confidentiality or obligations under the GDPR, not least because GDPR accepts that sensitive data may be processed if this is necessary for the establishment, exercise or defence of a legal claim (Article 9(2)(f)).

The legal importance of such medical notes in such circumstances was dramatically brought into the limelight in the case by the UK General Medical Council (GMC) against Dr Hadiza Bawa-Garba[22], who was convicted of medical manslaughter after a six year old boy died of sepsis which was not diagnosed by the doctor early on during his critical care. The facts of the case are not relevant to the discussion of this report per se, but the concern the case raised about the use of the doctor's own reflections in her e-portfolio (a part of the EHR), and her admission of culpability in those notes. Although the GMC made clear that the e-portfolio was not part of the evidence submitted to the court[23], excerpts from it were made available to expert witnesses and many commentators believe its content had an impact on the case[24]. Regardless of the material impact the e-portfolio actually had, the case makes clear that a medical record may concern more people than the patient, and may be of significant legal interest to people other than the patient. In the context of this report the case serves to remind the reader that the law of data protection in the healthcare setting sits within a complex system of other laws and interests so that data protection must be understood within the context of other rights and interests.

The way in which the right of access is in practice available to a patient will also be influenced by the way in which healthcare records are created and managed in a Member State, with countries with well-established EHR systems providing more simple means for patients to access and export records.

The data subject's right to access to health data concerning him or her

Grundstrom et al (2019) remark that they "consider access to be both an abstruse and intrinsic property of data that is enacted in various contexts by different stakeholders". These contexts, involving varying levels of complexity, emerge through stakeholder and technical interactions. They give an example from Denmark which runs as follows:

> *"Residents in Denmark have access to their health data through a central platform called Sundhed.dk. The act of a data subject (e.g. the resident) using this platform to find personal data is described as 'access', but a clinician may 'access' the same health data to make a diagnosis. These data can also be anonymised and 'accessed' by researchers for use in a clinical study."*

[22] R v Bawa-Garba (Hadiza) [2016] EWCA Crim 1841.
[23] https://www.gmc-uk.org/-/media/documents/ Factsheet___Dr_Bawa_Garba_case_final.pdf_74164961.pdf
[24] https://thehealthcareblog.com/blog/2018/01/30/to-err-is-homicide-in-britain-the-case-of-dr-hadiza-bawa-garba/

They conclude therefore that in this example there are three different stakeholders, three different reasons for access and three different types of access. This shows the need to clarify the way in which terms such as 'access' should be understood in the context of research.

In the survey the respondents were asked to reflect upon access to health data by data subjects, and asked to clarify how such access could be obtained, whether this was through direct reference of Article 15 GDPR or if special legislation has been adopted at Member State or regional level to facilitate access. As the right to access is codified in GDPR, all Member States assure this access, and correspondents report that in almost all Member States it is possible for patients to access their electronic health records electronically, either through a national ICT system or some regional or health service specific solution, although in about half of the Member States access is restricted to particular parts of the EHR.

Table 6.3 show shows that in the majority of Member State patients need to ask the data controller for access to data concerning themselves, and the controller will give such access based on the right under Article 15. In some countries a formal data access request system has been set up at national level.

Table 6.3 GDPR Article 15 stipulates that data subjects (including patients) have a right to access data concerning them. Please indicate the way in which this right may be exercised in your Member State.

How is patients' access to data concerning them facilitated?	Total MS	
Through a formal national data access request system established by legislation	9	AT, BE, BG, DE, EE, LV, HU, MT, SK
Through a formal regional data access request system established by legislation	0	
A patient needs to request access from the data controller by direct reference to Article 15 GDPR	20	AT, CY, DK, DE, EE, IE, EL, ES, HR, IT, LV, LT, LU, HU, MT, PL, PT, RO, SI, SE, [UK]
Other	8	CZ, DE, EE, FI, FR, LV, NL, SK

* For information per Member State, see Table A1.10 in Annex 1

The survey also asked more detailed questions concerning access to EHRs by patients. Table 6.4 below provides the details, showing that with respect to EHRs direct access through a nationally organised ICT system is the most common access route, with 22 Member States having adopted such at national level. Only 13 Member States this is to the full record, with the rest giving such direct access only to a partial EHR.

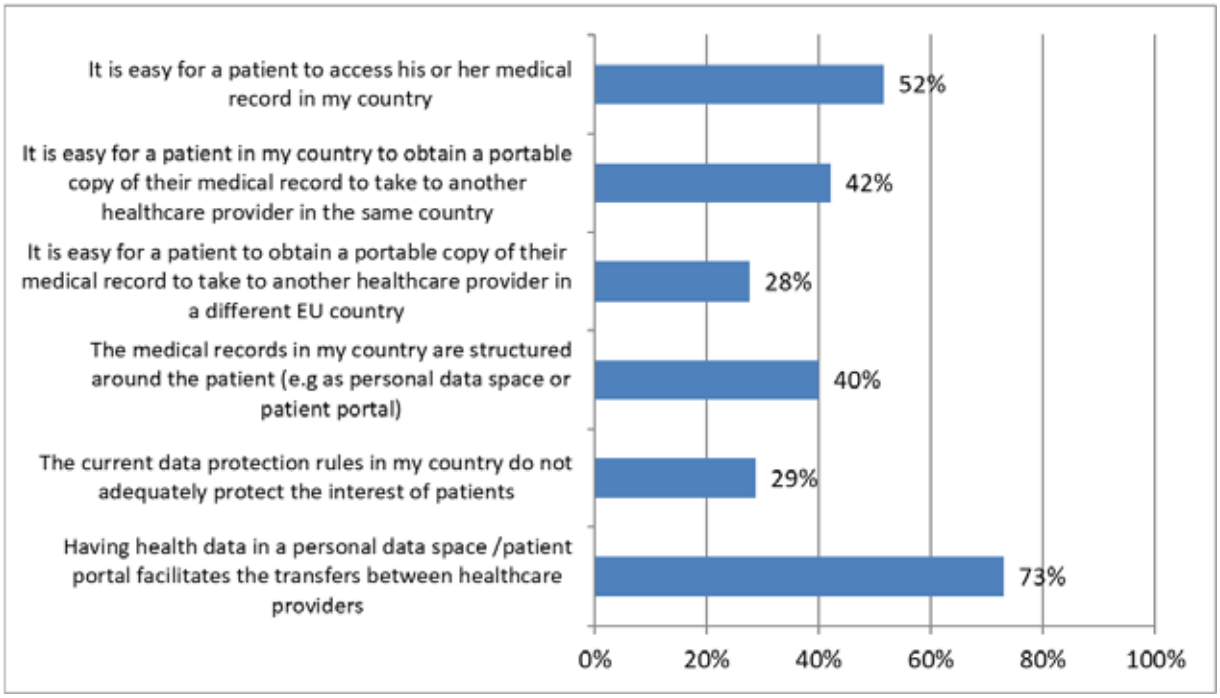
In order to better understand the nature of patients' access to data the survey also asked if patients could add to the EHR themselves. The returns show that only ten Member States allow such access (see Table 6.4, last two rows). The correspondents also report that in some of these Member States, citizens can request additions or changes, but they need to approach a healthcare professional to do so. In some Member States (such as CZ, NL), patients can add comments or change demographic data such as contact details, but cannot change health data themselves. Summarising, in most Member States there is at least some accessibility for patients to their personal data, however making corrections to their health data is not possible or can only be done through healthcare professionals in the majority of the countries.

*Table 6.4 ICT system through which **patients** can **access** their EHR data*

In your Member State, is there an ICT system through which patients can access their EHR data?	Total MS	
Yes, this is organised nationally	22	BE, DK, DE, EE, ES, FI, FR, HR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PT, RO, SI, SK, SE
Yes, this is organised regionally	5	BE, DK, ES, IT, SE
Yes, this is organised by individual health services	1	DE, [UK]
No, there are no such ICT systems	2	IE, EL
Other	5	BG, CZ, EL, LV, PL
If you answered yes above, do patients have access to the full EHR or just specific parts?		
Full EHR	13	DE, ES, FR, IT, CY, LV, LU, HU, MT, RO, SI, SK, SE
Partial EHR	11	CZ, DK, EE, FI, EL, HR, LT, NL, AT, PT, SE, [UK]
Can patients add data to their EHR?		
Yes	10	DE, EE, FI, FR, IT, LV, LT, LU, NL, PT, SK
No	16	BE, BG, CZ, DK, CY, HU, IE, EL, HR, ES, MT, AT, PL, RO, SI, SE, [UK]

While this is positive in that it reflects that the right to access is addressed in all Member States, it may also underline that access is not easy for patients, a point that was reflected also in the stakeholder survey, in which 52% indicated that they thought it was easy for patients to access data (implying that almost half thought it was difficult) and only 40% felt that the medical record is structured around the interests of the patient.

Figure 6.1 Share of stakeholder agreeing with the following statements, all related to the current situation regarding patients' rights



A good example of a Member State in which a simple access to EHR system is in place is Austria where the national EHR system (ELGA), which includes a formal national data access request system, established by legislation, by which all EHR participants are entitled either electronically by way of the e-Health access point (online patient portal) or by written statement to the EHR-ombudsman (as the analogue pendant) to receive full information concerning all their EHR data processed in ELGA, as well as all log data (who has accessed which of their EHR-data when, for how long and according to which search criteria). In the Netherlands the patient can access his medical records at each health care provider and has a right to access the log as to which professionals have accessed this information. However, while some Member States have clearly invested heavily in making access to EHRs simple and user friendly, or made this an obligation for health care providers, the fact that only half of the stakeholder respondents reported that they found access easy suggest that more could be done to make that right easily exercisable for data subjects with respect to the health-related data about them held in various parts of the healthcare systems of the EU Member States. The challenge here is however more likely to be one of technical and legal interoperability, rather than creation of new legal tools.

The data subject's rights to rectification and to restriction of data

The GDPR also conveys the rights of rectification of incorrect data on a data subject. The right to restrict the processing of certain data will be used when the right of rectification is in process and not yet complete, so that data processing is limited while the rights are executed. With respect to the exercise of the right to rectification in the health sector, such a request follows the way in which the Member States provide for the exercise of rights in the health area.

Most Member States use a combination of specific legislation in the area of health and the direct application of GDPR, that is a patient who wishes to have health related data corrected may do so through specific legislation or through reference to the GDPR. The survey also asked correspondents to report if the Member States had adopted any legislation pursuant to Article 23 that could limit the right of rectification in the area of health, distinguishing such limitation from the measures adopted under Article 89(2) with respect to data used in research.

Table 6.5 Article 16 of the GDPR requires that a data subject shall have the right to rectify any inaccurate data concerning him or her. Please indicate how this operates in your Member State.

Art. 16 data subjects' right to rectification	Total MS	
Through a formal national data rectification request system established by legislation	6	BG, DE, LV, HU, MT, SK
Through a formal regional data rectification request system established by legislation	1	FI
A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR	22	BE, DK, DE, EE, IE, EL, ES, FR, HR, IT, CY, LV, LT, LU, HU, MT, AT, PL, PT, RO, SI, SE, [UK]
The right to rectification is restricted based on sectoral legislation adopted in accordance with Article 23(1)	7	CZ, DK, DE, FR, NL, AT, SK

As table 6.5 shows, the right to rectification would appear limited in seven Member States, and in each case this limitation is based on the justification that the medical record must remain a complete record of all events and encounters between the patient and the healthcare system. Rectification is therefore limited in such a way that a note

may be added to the record stating that the patient wishes information to be recorded, but not obscuring the previous record. In some cases, the EHR systems allow for a patient to do these themselves within the system, while in other cases a healthcare professional has to enter the note. In some countries the rules vary based on the nature of the information to be rectified, thus in FR 'material' information such as names, addresses etc. can be changed whereas 'medical' information cannot. In other countries even such 'material' information is recorded as a new entry, rather than a correction.

Erasure of data from a health record

When the GDPR was enacted much publicity was given to the fact that it created a 'right to be forgotten', that is, a right to have certain data deleted from records. The right as set out in Article 17 is however limited when it comes to health-related data, as the legislators recognised in Article 17(3)(c) GDPR that the right should not apply for reasons of public interest in the area of public health pursuant to Article 9(2)(h) and (i) and Article 9(3). In this respect, account must be taken that a health record has a wide impact and it may not be appropriate to remove any entries from the full record. This may be for legal reasons, both for the protection of the patient and the people involved in treating the patient, but may also be to ensure that future healthcare professionals have available all facts that may define treatment options. Health records may in certain circumstances have a wider public health importance, both for specific research projects as well as for health system planning, defined as three distinct functions as discussed in the preceding chapters.

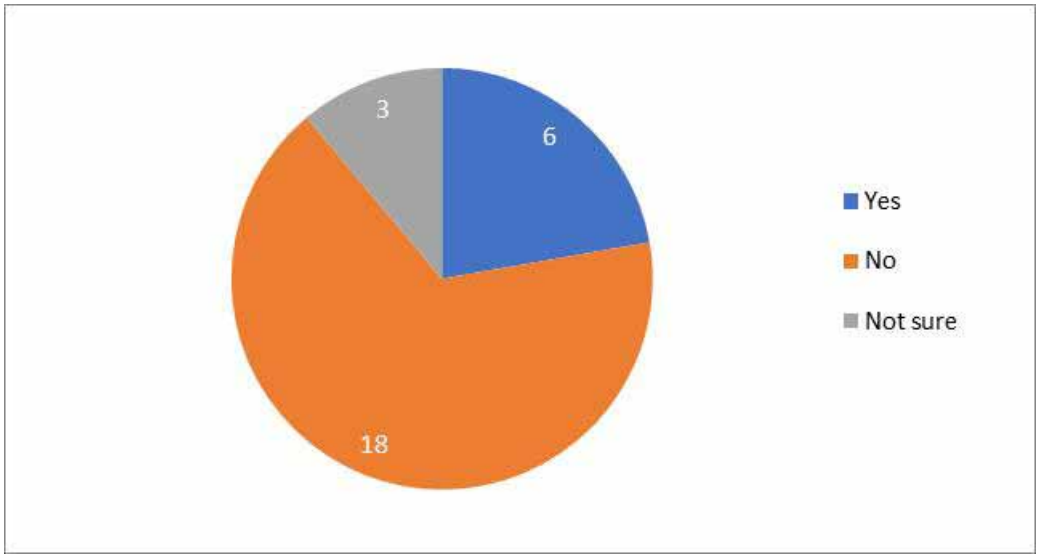
The right to erasure will usually arise with respect to health related data if the data subject withdraws consent, when consent was the legal basis of data collection and processing, or in cases where the data processing in question is unlawful. GDPR expressly provides in Article 17(3) various exemptions to the right to erasure, such as in so far as necessary for reasons of public health in accordance with 9(2)(h) and 9(2)(i) GDPR as well as 9(3) or for scientific research purposes in so far as the right to erasure would render impossible or seriously impair that objective. In addition to these exemptions, Article 23 provides that Member States may adopt further legislation limiting the right to erasure if there is a general public health interest in doing so. Noting these limitations on the right to be forgotten in the healthcare setting, the survey asked if patients had a right to have records deleted. The correspondents reported that this right does not exist as an absolute right in any Member State, and never arises in seventeen countries. In nine countries, however, such deletion was reported as being possible in certain circumstances. The correspondent for Sweden, for example, noted that this could only take place based on a decision of the Health and Social Care Inspectorate after an application by the patient. The correspondent commented that success was likely to be very rare, but noted that such a decision could be appealed to the General Administrative Court. For France it was noted, in line with the comments on rectification, that some parts of a record may under certain circumstances be deleted, but not the whole record. In the Netherlands the entire medical record may be deleted upon request of the patients, unless the legitimate interests of others to maintain it outweigh the interests of the patient. There is no case law known where a court had to decide about this balancing when a record had not been deleted so these requests are presumably rare.

Table 6.6 Art. 17 data subjects' right to be forgotten

Please indicate if a patient may have medical records deleted in your Member State (based on Art 17)	Total MS	
Yes, always	0	
Yes, but only under certain conditions	9	DE, IE, ES, CY, LT, LU, NL, PT, SE
No	16	BE, BG, CZ, DK, EE, EL, FR, HR, IT, LV, HU, AT, PL, SI, SK, FI, [UK]
Not sure	2	MT, RO

To explore the idea of partial deletion further, and to investigate the patient's interest, the survey asked if a patient could request the removal of specific health data concerning cured diseases (e.g. cancer) from his or her electronic health record. In response six countries are shown as allowing this to happen (see Figure 6.2 and Table A1.16 in Annex 1). Account must be taken that in several countries national legislation exists which requires the retention of such data for a certain length of time. In Spain this arises only if at least five years have elapsed since discharge, although this period may be longer if legislation of the autonomous regions so provides. In Italy data may be obscured, but not fully deleted, as it must remain accessible to the party who generated the data, usually the treating physician; while in Lithuania the right is similar but the full record must remain visible to the family doctor as well as the party who generated the data. In Austria the healthcare providers can delete electronic references to the respective health record stored locally (so that the data cannot be accessed in the EHR (ELGA) system anymore), but not the local record itself due to the minimum retention periods for medical documentation necessary for compliance with a legal obligation.

Figure 6.2 Does your Member State allow that a patient request the removal of specific health data concerning cured diseases (e.g. cancer) from his/her electronic health record?



* For information per Member State, see Table A1.16 in Annex 1

6.2.3. Data Portability

With respect to healthcare provision the right to portability is perhaps the most important right from a patient perspective, since it supports the patient in seeking care from a new healthcare professional in his or her own Member State as well as in other countries. The GDPR creates a general right of portability of data in the following situations: when the data have been collected on the basis of consent or contract and where the data are processed by automated means. Portability demands that an organisation provides the personal data in a machine-readable format on request by the data subject. However, there are difficulties around the process of ensuring data subjects' knowledge of their right to portability and the lack of digital standards for formats to allow portability in a machine-readable format to be realised.

The table below shows that the right to portability of health data can be exercised in all but four countries - however, this does not mean that it is easy for a patient to exercise that right. In five Member States (DK, LV, SK, RO, SE) the right as set out in GDPR is not generally applicable because the data are not collected on the basis of consent or contract. In response to a further question on how EU action could support portability of health data, some indicate that greater support for use of standards for data processing and security would be helpful, while others mention the value of monitoring and reporting on the exercise of this right.

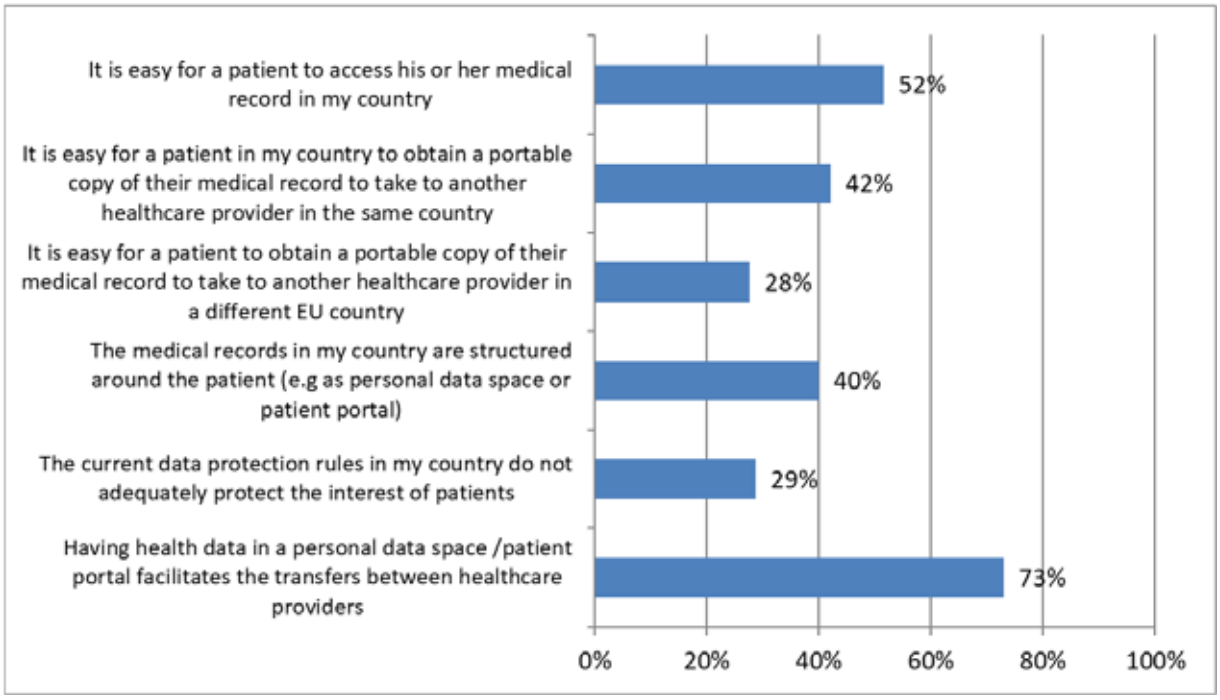
Table 6.7 GDPR Article 20 stipulates that if the data collection was based on consent or on the basis of the creation or execution of a contract, the data subject (patient) has a right to obtain a portable copy of the data. Please indicate which of the following apply in your Member State.

Art. 20 data subjects' right to data portability	Total MS	
through a formal national data portability request system established by legislation	6	BG, DE, CY, EE, HU, AT
through a formal regional data portability request system established by legislation	1	IT
A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR	17	BE, DE, EE, IE, EL, ES, FR, HR, LT, LU, HU, MT, NL, PL, PT, SI, FI, [UK]
Patients cannot obtain a portable copy of medical records (Article 20 does not apply because data is not collected on the basis of consent and no sectoral legislation allows this)	5	DK, LV, SK, RO, SE
If you have selected the last option above please describe why Article 20 does not pertain to patient data:		
Article 20 GDPR does not apply because health data are not collected on the basis of consent	4	DK, LV, SK, SE
Article 20 GDPR does not apply because data processing is not carried out by automated means (e.g. no Electronic Health record)	2	LV, RO
Because legislation pursuant to Article 23(1) has been enacted which limits the scope of the data subject's (patient's) rights.	0	
Other reason	1	SK

Stakeholders' comments on patients' right to data portability

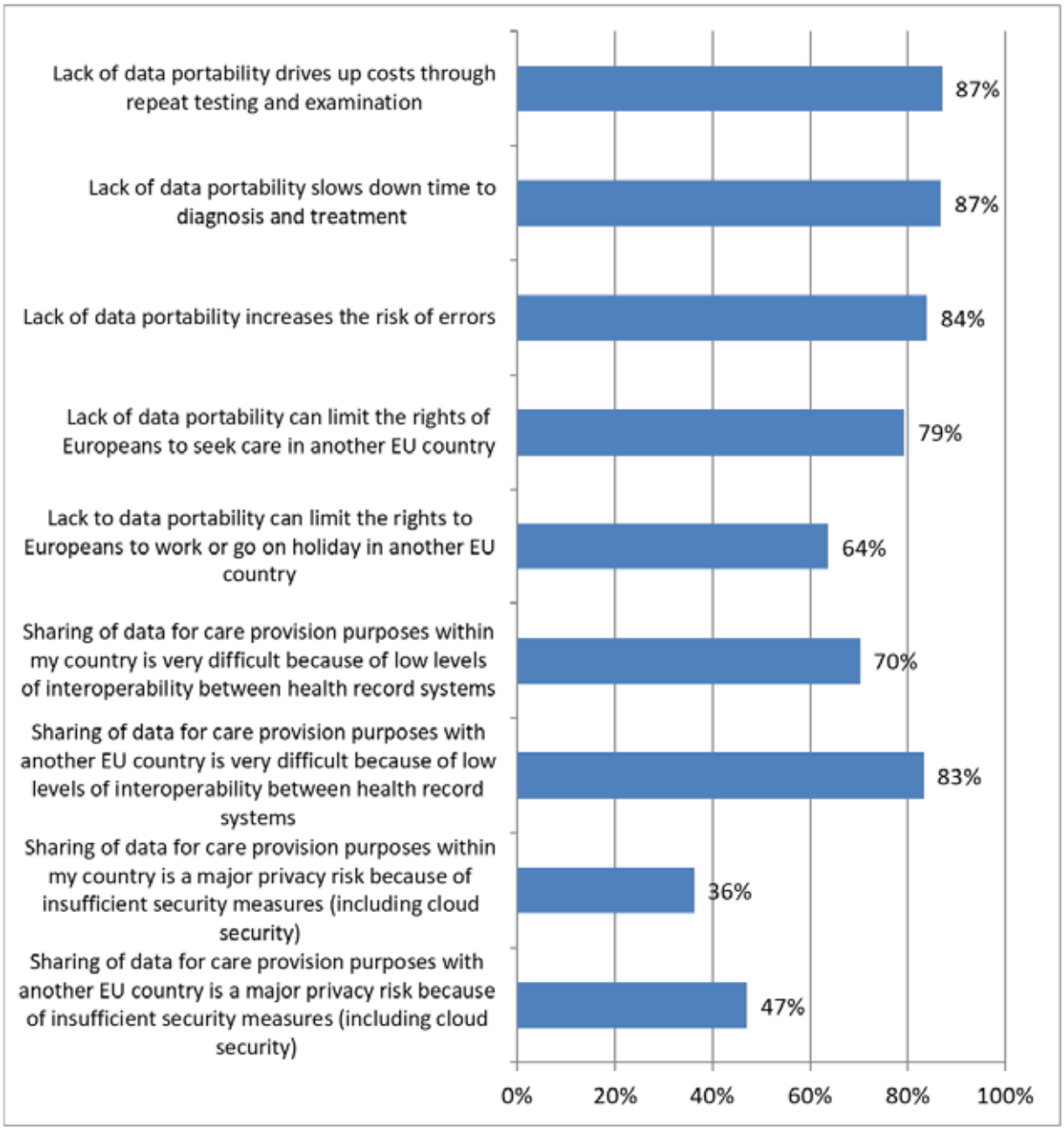
The issue of portability of health data was also raised in the stakeholder survey, including in a number of questions on possible further EU level action. The survey identified that 40% of the respondents indicated that medical records are accessible in a personal data space or patients' portal, and only 28% of all respondents believed it was easy to make such a portable record available to another healthcare professional in a different EU Member State, while 73% felt that having health data in a personal data space /patient portal facilitates the transfers between healthcare providers.

Figure 6.3 Share of stakeholders agreeing with the following statements, all related to the current situation regarding patients' rights



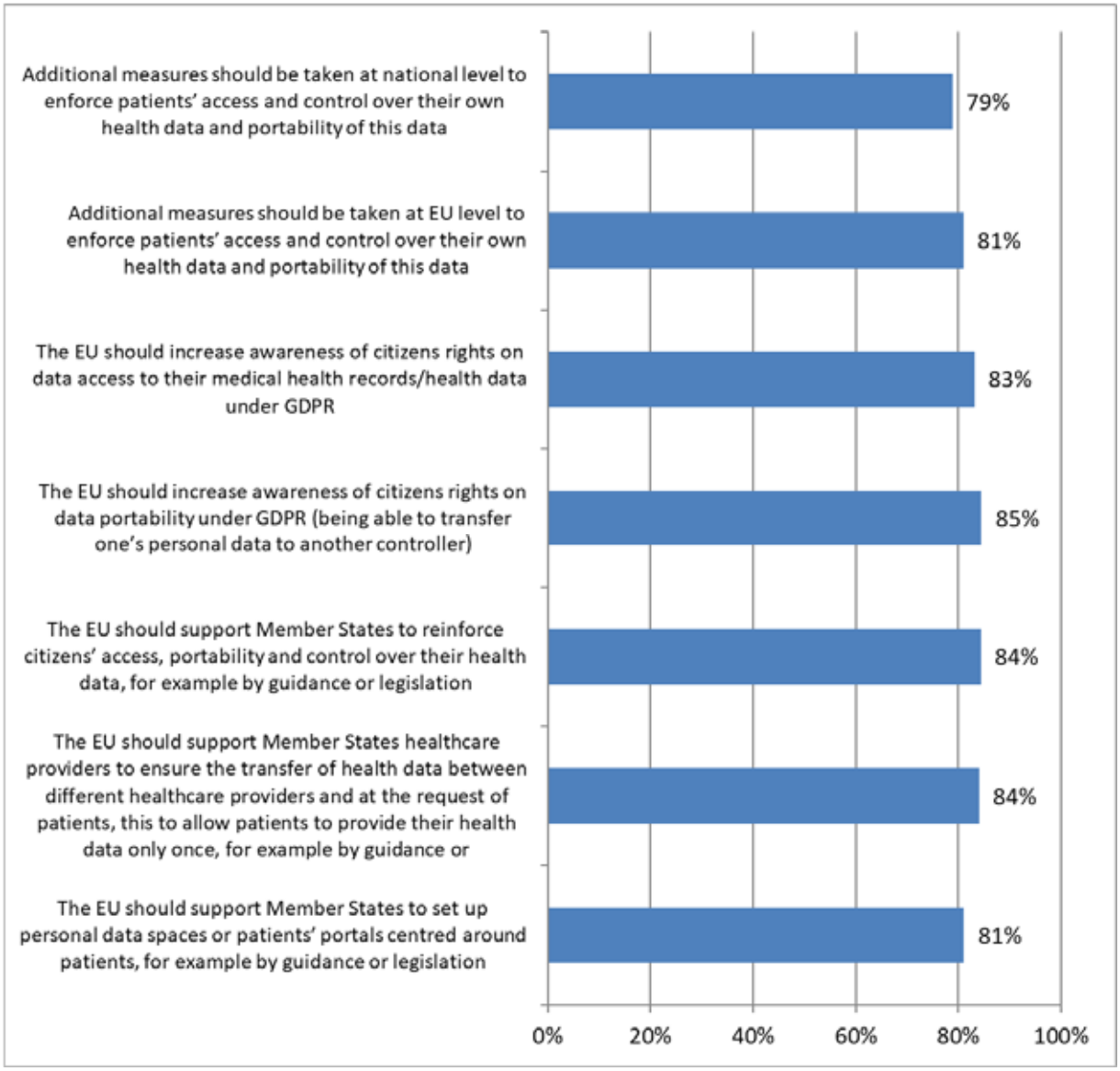
Further responses indicate that the respondents felt that the lack of ease in exercising the right of portability has a negative impact on healthcare systems, on patients and on citizens, among others by driving up costs, slowing down time to diagnosis and treatment and increasing risks of errors. Similar to the findings of chapter 3, one of the main barriers is that sharing of data for care provision purposes with another EU Member State is seen as being very difficult because of low levels of interoperability between health record systems (with 83% agreeing with this statement, see Figure 6.4).

Figure 6.4 Share of stakeholders agreeing with the following statements, all related to the way in which data sharing for providing care is possible



To circumvent these risks and difficulties a majority of stakeholders also agrees that action should be taken at EU level (Figure 6.5). It refers among others to the role of the EU in increasing awareness on citizen rights and supporting Member States to reinforce citizens' access, portability and control over their health data. A majority (81%) also supports the notion to set up personal data spaces or patients' portals centred around patients, for example by guidance or legislation.

Figure 6.5 Share of stakeholders agreeing with the following statements, all related to whether patients' rights should be improved



6.3. Concluding remarks

The surveys as well as the workshops indicate that while the Member States respect all the requirements of the GDPR with respect to data subject rights, the extent to which such rights are truly exercisable by patients may still have some way to go. Although some limitations and barriers are required in a healthcare setting, such as the requirement to maintain a complete record of healthcare interventions so that future care decisions are evaluated on the basis of all relevant information, the exercise of the rights of the data subject in the healthcare setting remain limited. This arises both because suitable policies have not been adopted and because of practical implementation. The European Patients' Forum noted in its submission to the European Commission's consultation on the Data Strategy that access to one's personal data, exercising control over data, transparent information about processing, and the right to be forgotten or to erase data all still require more action to ensure that the duties of data controllers are effectively implemented, and that data subjects (patients) are supported with patient friendly information and transparent processes (European Patients' Forum, 2020).

On the matter of the right to data portability, it is worth noting that the current practical barriers largely result from the low level of use of standardised EHRs as well as the low level of awareness among patients of their rights. The stakeholders' responses clearly indicate that they believe patients' rights with respect to control of their data should be addressed both at national level and EU level, while over 80% believe that the EU should actively engage in supporting Member States to make those rights better known and more realisable. It is worth considering also if action should be taken at EU level, in particular with respect to the rights of data access and to portability. This will be addressed in greater detail in chapter 8 (Section 8.4).

7. DATA GOVERNANCE STRATEGIES AND BODIES

The purpose of this chapter is to consider in greater detail the existing governance structures and strategies for managing health data that exist in the Member States, with a particular focus on re-using data for research purposes (function 2 and 3). We will look at national agencies or bodies authorised to grant permits for the use of data already collected for another specific purpose, as well as any other mechanisms for providing access to health data for research and public policy purposes, including by means of initiatives to further enhance data altruism**.** This will help to identify possible options for improvements in effectiveness, efficiency and coherence of systems for providing access to data for secondary uses, and draw out recommendations for further action at EU level to support access to health data for secondary uses in the context of the creation of a future European Health Data Space as set out in the European Digital Strategy.

7.1. Regulatory mechanisms which address the use of health data for research purposes

Approval mechanisms to allow access to health data for secondary purposes can take a variety of forms, which may be defined by the nature of the research to be undertaken, the nature of the data to be used, or nature of the researcher. In some cases, the nature of the research will define if sectoral law applies, for example, data processed in the context of a clinical trial are regulated by Directive/2001/20/EC on Clinical Trials (soon to be replaced by the Regulation 536/2014/EU on Clinical Trials). However, when the research takes place in a clinical study not covered by the law on clinical trials, such as observational research, the GDPR and its Member States implementation will govern the way in which access to data is controlled. In addition to EU level legislation, national rules on the operation of research ethics committees may also apply, as well as the rules governing the national level data clearing houses, such as the French Health Data Hub or Finland's Findata. It is important also to note that the provenance of data to be used in research is also significant in understanding how rules will be applied. When data are collected *specifically for research*, hence when research is the primary purpose, the purpose must be described to the data subject, including any potential further research which may be undertaken beyond the primary project. In this sort of situation, the legal base for data processing will often be consent (Article 6(1)(a) and 9(2)(a) GDPR); although other legal bases may also be used.

However, the primary interest of this chapter is on the secondary use of data for research. Such processing may be classified as 'further processing' of data, and as such may be prohibited under the GDPR, because, as noted in chapter 5, data may not generally be subjected to further processing in a manner that is incompatible with the purpose stated at the time of collection (Articles 5(1)(b) and 6(4) GDPR). However, where the further processing is for research purposes, Article 5(1)(b) states that such further processing is not always considered incompatible; it demands however that such further processing for research is safeguarded in accordance with Article 89(1) (see box 5.1).

Given that the GDPR has only applied for two years, there is only limited jurisprudence on the application of the research relevant articles. However, as already noted in chapter 5, the *Preliminary Opinion on data protection and scientific research* issued by the European Data Protection Supervisor in January 2020 (EDPS 2020), draws a distinction between 'genuine research for the common good' and 'other research which serves primarily private or commercial ends', with the distinction between the two having become ever more blurred. While it does not offer a definition as such, it notes that

'independent ethical committees could support the understanding of which activities qualify as genuine research and define the ethical standards referred to in the GDPR'.

7.1.1. Main types of application procedures for data access

In order to better understand how the articles and derogations which allow the further processing of data for research are implemented in the Member States, the survey completed by country correspondents explored how access to health data for further research purposes is organised and the extent to which special mechanisms have been set up to facilitate access to data. In contrast to the reporting of the responses to the survey in chapters 3-6, in this chapter we created composite tables showing responses across several questions. Table 7.1 below shows the access mechanism reported as having been adopted in each Member State.[25]

*Table 7.1 Access mechanism for secondary use of health-related data**

Access mechanism for secondary use of health-related data	Total MS	
Access is granted after authorisation by research ethics committee (REC) or data protection agency (DPA)	22	BE, CZ, DK, DE, EE, IE, EL, ES, FR, HR, IT, CY, LV, LT, LU, HU, AT, PL, PT, RO, FI, SE, [UK]
The data controller provides direct access without engagement of an ethics committee or DPA being required	7	DK, HR, IT, NL, AT, SI, FI, [UK]
Centralised governance body exists in some form	13	BG, DK, DE, IE, EL, FR, CY, MT, NL, PT, SI, SK FI, [UK]

* Some countries may have different mechanisms for different types of data, research and/or researchers and thus may appear in multiple rows in this table.

The first point of note is that all Member States reported to have created some form of mechanism for researchers to gain access to at least some types of data previously collected for other purposes, although in some cases this may be to only a limited category of data. As indicated in the table, almost all the Member States use some form of Research Ethics Committee (REC) either at national or regional level, and in some cases the RECs also provide the necessary approval for data to be made available through a centralised data governance and access body. The notes provided by correspondents indicate that usually the DPA and REC processes happens in tandem. REC approval is an ethical requirement as established in international law. Some jurisdictions have specific legislation requiring REC approval before research can begin while in other countries it is an ethical or policy requirement (rather than a legal one).

Ordinarily there is interaction between both REC and DPA during the approval process. Once REC and DPA approval has been received the research and data access can begin.

[25] Tables 7.1, 7.2 and 7.3, which are discussed in further detail in this table, have been created using the responses to questions 37, 38, 41, 74-85 of the survey completed by country correspondents. In some cases the authors of this report allocated a country to a category based on the notes of the correspondents and further desk research. Latvia, for example, has been allocated the category of using REC or DPA approval as opposed to 'other' as originally indicated. This is because the detailed response shows that in Latvia access is granted through a special committee of Centre for Disease Prevention and Control (SKPC) as provided for in Section 10, Paragraph eight, Clause 2 of the Law On the Rights of Patients, rather than a traditional REC, however for the purposes of this report that committee has been treated as performing the same function as a REC and so Latvia was allocated to that category.

The notes also make clear that the route to be followed will in many cases be defined by the nature of the research, the data, or the organisation conducting the research. In Denmark, for example, application to the local or national research ethics committee is required where the research directly involves patients or tissue samples. However, where the research is on data only, approval of a REC is not usually needed. The correspondent for the UK notes that if the data to be used are data that were originally collected for care provision purposes, the approval of a REC is not needed where the data have been anonymised; however REC approval is always needed if the data are collected expressly for research.

It should be noted that this is a changing landscape, with a number of Member States initiating changes in legislation and operational procedures. In the case of Italy, for example, proposals have been made to establish centralised data access procedures in the context of Italian research hospitals (the Istituti di Ricovero e Cura a Carattere Scientifico, IRCCS), but a single national entry-point has yet to be implemented. It is significant also that correspondents from eighteen Member States reported that exchange of health data for both care and research was made more complex in their views by the fact that a wide range of governance models exist across the Member States, and they generally felt that neither the legislation in the Member States nor at EU did much to facilitate data exchange between Member States.

7.1.2. Access to data where no centralised national system exists

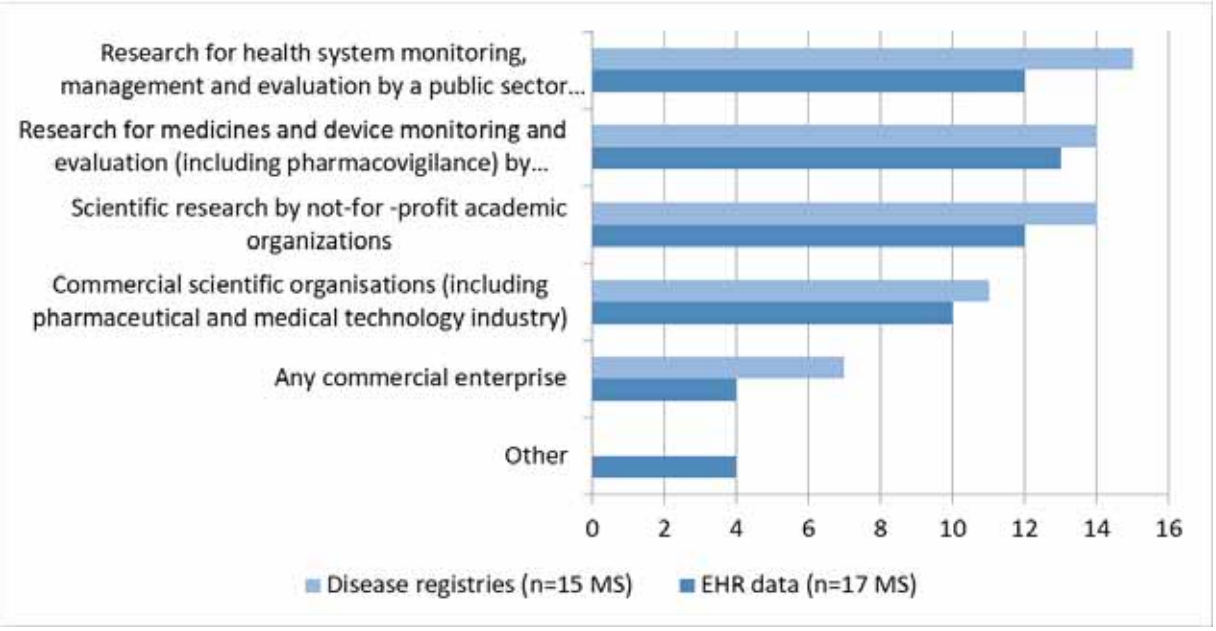
Table 7.1 above shows that thirteen of the country correspondents indicate that their Member State has some form of centralised data governance access body, although as noted in some cases this is limited to a very narrow range of data. While these cases will be described in greater detail in section 7.3, this does not mean, of course, that in the remaining EU Member States secondary research with health-related data is not possible. For instance, in a large number of cases, a central body such as the national statistical office and/or the national institute of public health provides some form of access to (mostly aggregated) health data, with steps being taken to enhance the availability of personal health data as well. E.g. in Romania data storage is managed by the National Health Insurance House (CNAS), including data from EHRs (at http://www.des-cnas.ro), but as the system is not yet functional, there is currently no procedure applicable for researchers. In addition, other routes may exist, and indeed in some cases, as shown for Denmark above, such routes may exist alongside a centralised system. Another example is Sweden which is listed as not having a centralised data access infrastructure, but which does have other bodies fulfilling such a role. For example, the Stockholm Centre for Health Data which started operations on 1 October 2020, will perform a service role for those who are entitled to gain access to health data from the Stockholm region for research and development purposes.[26] In comparison, while Italy presently lacks a single entry point for data re-use for research purposes, it does have several regional systems and several sector specific systems (e.g. hospital care networks, primary care networks) to share data for secondary use, with each region having its own system for transferring data collected within EHRs (the Fascicoli Sanitari Elettronici - FSE). The correspondent notes, however, that access to such data is not straightforward because there are no web portals through which researchers across the Member State or Europe can request access to data. Accordingly, access to such data seems to hinge on inside knowledge by national level researchers, often limited to their field of research.

[26] The centre assists healthcare providers by offering a one-stop-shop, not by having its own database, rather, it will coordinate the release of data for purposes permitted under applicable confidentiality and data legislation.

In countries where no centralised infrastructure exists, researchers can generally apply for access to data held in EHRs for secondary use by contacting the data controller (the healthcare provider or professional that collected the data). In six of these Member States, in addition an application should be filed with a research ethics body (see Table A1.32, Annex 1). The national Data Protection Authority appears to be seldom involved in this application procedure. Only Cyprus and France report having a combined application system to a local/national ethics committee and the DPA. Austria also indicated that applications can be made to the DPA, but as clarified by the Austrian consultant such involvement is only a subsidiary tool under Art. 7 of the Federal Act on the Protection of Personal Data (DSG). Moreover, under the more recent and more specific Federal Act of Research Organisation Act (FOG) there remains only an even smaller scope for involvement of the DPA, e.g. in cases where the researcher is no scientific institution according to Art. 2c (1) FOG.

In order to better understand how EHRs and disease registries are used as data sources when no centralised system exists, correspondents were asked series of questions about access to each of those sources for secondary research (although the difference between both is to some extent arbitrary, as some disease registries are based on EHRs). Their responses are mapped in Figure 7.1 which demonstrates very well that even without a centralised data governance system a wide range of research is possible. It would seem however that industry is less well served in countries where there is no centralised data governance system. The 'public interest' criterion which is in many legislations a condition to legitimise the intended research, will play a role here, and which may have been addressed when creating new infrastructures specifically to support research.

*Figure 7.1 Types of research that may be conducted using data held in EHRs and disease registries (for Member States with **no** centralised data access infrastructure)*



* For information per Member State, see Table A1.33 in Annex 1

7.2. Access to data where some form of centralised national system exists

Of particular interest to this study are the 13 Member States listed in Table 7.1 as using some form of centralised data governance organisation (BG, DK, DE, IE, EL, FR, CY, MT, NL, PT, SI, SK and FI). Seeking to gain more insight into how these bodies operate, a series of questions was asked about such infrastructures, including the sources of data they use, their legal status and organisation, fees paid etc.

First, in section 7.3.1 we give an overview of the relevant bodies, accompanied with a summary description for each. Next, in Section 7.3.2 we provide a more extensive description of all bodies. It is important to add that the distinction between the 13 Member States listed here versus the 14 other Member States is not that clear-cut. The reports of the correspondents indicate that multiple routes to access data continue to exist in many Member States; having a central data access body thus does not mean that it is an *exclusive* access body. E.g., as the case of Finland in Box 7.1 clarifies, a Member State may have one central body in place (Findata), but if data is needed from only one data controller, then that single data controller may give permission to the use of that data instead of Findata. In addition, Member States that listed not having a centralised data access body may still operate some form of data access infrastructure at national or regional level. Instead of a dichotomy between Member States with and without centralised access bodies, it may be more appropriate to consider them as being placed on a continuum with some Member States such as Finland having a strongly developed centralised data governance system, while in others the central governance models that do exist are more light touch, often in line with the nature of the health system as a whole.

7.2.1. Main characteristics of data access bodies

Box 7.1 below sets out a description of the centralised data governance systems in the thirteen Member States for whom the correspondents indicated such a structure, or where interviews with key actors as well as desk research indicated the existence of such a structure. The overview below is not intended to give a complete overview of all relevant governance bodies in a Member State, but rather describes the main body that currently has a central role, often existing in parallel to other bodies and data controllers that are in place. The Box also shows that in some countries governance is arranged in more institutionalised public formats while other Member States rely more on within-sector governance.

Box 7.1 Overview of access and governance bodies in all 13 Member States*	
Member State	**Institute, short description, website**
Bulgaria	The **National Centre Of Public Health And Analyses (NCPHA)** provides statistical information following the Health Act (HA) and the Personal Data Protection Act. A written application can be made to provide access to data by the NCPHP, but to date this is limited to public information. Website: https://ncpha.government.bg/en/
Cyprus	The **Ministry of Health** and the **National Bioethics Committee** evaluate research applications made. The National Bioethics Committee consists of three Review Bioethics Committees, that review protocols relating to: • biomedical research on human beings and their biological substances • clinical trials on Medicinal Products for human use, and, • Medical devices applied on human beings Even for pseudonymised data, the National Bioethics Committee needs to provide the researcher with a decision whether there is a need for full application of ethics. Researchers need to attach the decision of the National Bioethics Committee to their application to the Ministry of Health. Application fee is 50 Euro. Other than this, there is no fee payable. http://www.bioethics.gov.cy
Denmark	The two main national data governance bodies that host health data are: **Statistics Denmark** (storing data about the wider Danish population) and the **Danish Health Data Authority** (hosting disease registers and databases with health related information) (see also section 7.7 for a detailed description). Researchers can apply for access to data locally with data custodians, or for the whole country either through the Researcher Service (Forsker-service) at Serum Institute (when it is health data only) and through Statistics Denmark, if the researcher wants to combine health data with other data types. Websites: Statistics Denmark https://www.dst.dk/en and Danish Health Data Authority https://sundhedsdatastyrelsen.dk/ Note. To illustrate the complexity of the landscape, the correspondent for Denmark clarified that as Denmark has a highly developed ICT infrastructure, it also has multiple systems developed to serve different clinical needs, and not all of them go through the main national infrastructural access points (Sundhed.dk or Statistics Denmark). For example, KiaP (Quality in General Practice) provides access to general practice EHR data for research, while for the five Danish Regions a cross regional network organisation was set up regarding the use of data in a vast number of regional quality assurance data bases, called the RKKP (the Regions Clinical Quality Assurance Program). Access for researchers in these data is coordinated by the RKKP, with the decision regarding access is made by the steering group of the individual data base in the RKKP.
Finland	**Findata** is an independent central agency which operates under the performance management of the Ministry of Social Affairs and Health (see also section 7.7 for a detailed description). Findata provides access to health and social data, develops and guides Findata's operations. The Data Protection Ombudsman, Parliamentary Ombudsman and Valvira* supervise the operations of Findata and compliance with the Secondary Use Act and data protection legislation. Permits can be obtained for the secondary use of personal data. For statistical data, access is provided based on a data request. Findata issues permits for obtaining personal data in cases involving secondary use of health and social data, and combining data from registers of multiple controllers or obtaining data from private social welfare and health care service providers. In such cases, access is granted via

	a remote access to a secure environment maintained by Findata (unless transferring of data is absolutely necessary). Fees apply for the application procedure, which include the costs of data controllers to extract the data, working hours of Findata personnel for processing the data and for the remote access environment. Data requests are currently possible only with a Finnish personal identity code through Suomi.fi identification. https://www.findata.fi/en/services/services-for-customers/ https://www.findata.fi/tietoa-meista/ * Valvira is a national agency operating under the Ministry of Social Affairs and Health, charged with, amongst others, the supervision of the social and health care.
France	The **Health Data Hub** builds on previous initiatives and is set up as the single entry point for health data access in France providing access for all researchers to data currently stored in the Health Data Hub (see also section 7.7 for a detailed description). It is also responsible for health data access governance as it hosts the secretariat of the CESREES, the ethical and scientific committee for health research, studies and evaluations, which evaluates requests for access to the data catalogue. The Health Data Hub is both affiliated with the Ministry of Solidarity and Health and with the Ministry of Research. The missions of the Health Data Hub are determined through Article L. 1462-1 of the Public Health Code. The health data platform, with its governance set up by decree, is composed of 56 entities that represent, among others, the State, organisations ensuring representation of patients and users of the health system, producers of health data, public and private users of health data, including health research organisations. Website: https://www.health-data-hub.fr/
Germany	The **Research Data Centre at BfArM** (Federal Institute for Drugs and Medical Devices), supported by the Federal Ministry of Health is currently being set up (see also section 7.7 for a detailed description). Researchers can apply at the Research Data Centre to access data that BfArM holds, covering records of citizens with statutory health insurance. As of 2023 it is expected to provide access to EHR data for which patients will be able to grant access to. Website: https://www.bfarm.de/EN/ (until a new dedicated website is established) In addition, the Federal Ministry of Education and Research is setting up a **National Research Data Infrastructure (NFDI)** for the entire research landscape. The NFDI will act as national repository and systematically manage scientific and research data. It provides long-term data storage, backup and accessibility, nationally and internationally. Using a budget of 90 million EUR from 2019-2028, the NFDI will bring stakeholders together in coordinated consortia tasked with providing science-driven data services to research communities. The first consortia are starting in October 2020, including for health data a) a National Research Data Infrastructure for Personal Health Data, NFDI4Health and b) a German Human Genome-Phenome Archive (GHGA). Website: https://www.nfdi.de Third, is the **Medical Informatics Initiative (MII)** as set up by university medical sites. MII creates a harmonized framework for nationwide access to the exchange and use of patient data and biomaterials for medical research. Participating sites have agreed on a comprehensive model of usage regulation for the exchange of patient data, biomaterials and analysis methods and routines, among others providing uniform application procedures and transfer points at all participating locations, which guarantee secure data transfer. Website: https://www.medizininformatik-initiative.de
Greece	In Greece, **IDIKA S.A.** (e-Government Centre for Social Security Services) is an

	agency supervised by the Greek Ministry of Labour, Social Security & Social Solidarity, responsible for access to health insurance claims data, prescribing and dispensing data, and disease registry data. Information is accessible for all types of organisations. Law 4600/2019 Article 84 (11) states that the agency is allowed to publish or grant, on a subscription or special fee, statistical data, from which the data subjects can no longer be identified and which come from the operation of the archiving system of the Individual Electronic Health Record. The data access organisation is financed by the government. Website: http://www.idika.gr/
Ireland	The **NREC COVID19 (National Research Ethics Committee (NREC) for COVID-19** is a temporary committee to deliver an expedited process for review for all COVID-19-related research studies. It is installed as part of Ireland's response to the COVID-19 pandemic. In accordance with the WHO roadmap for R&D the Minister for Health established the National Research Ethics Committee (NREC) for COVID-19 to deliver an expedited process for review for all COVID-19 related research studies. The temporary NREC COVID-19 is designed to include structured and coordinated interaction with other bodies involved in regulation of health research including the Health Products Regulatory Authority (HPRA) and the Health Research Consent Declaration Committee (HRCDC). In this way, researchers and sponsors can expect to receive all the necessary decisions from appropriate parties within the same expedited timelines. The ambition of the NREC COVID-19 is to relay decisions back to researchers within 7 days of confirmation of a validated application. An application form must be completed which includes review and feedback on the study by the relevant local Data Protection Officer. A data impact assessment must be included where necessary. No fee is applicable, and once in receipt of approval from NREC COVID-19 the study can proceed, with access to data being granted by each relevant data controller. Website: https://www.hrb.ie/covid-19-ethical-review/nrec-covid-19-overview/
Latvia	The **Centre for Disease Prevention and Control (SPKC)** has a delegated function to issue a permit for the use of patient data recorded in medical documents in a specific study. The examination of the application and the decision on the issuance of the permit shall be performed by a specially established SPKC commission. Pursuant to a four party cooperation agreement (between the Centre for Disease Prevention and Control, the National Health Service, the Emergency Medical Service and the Health Inspectorate) on the establishment of a health care quality and efficiency monitoring system, a database has been created linking data from the above institutions. Provision of statistical and research data from the information systems of the Centre for Disease Prevention and Control is free of charge, except in the case that additional data processing or special data selection techniques are required to prepare the requested data have to be performed on the data by SPKC (https://spkc.gov.lv/lv/par-SPKC/pakalpojumu-cenradis). *Note that the Latvian correspondent indicates that the SPKC's functions fitting with a "centralised data governance and access body" only exist to some degree and in some cases.* Website: https://www.spkc.gov.lv/lv
Malta	The **Ministry of Health, Department of Health Information and Research (DHIR)** hosts health data available for research purposes, this as part of an e-health network of multiple data controllers. Data concern primary and hospital care electronic health records, disease registries and linked health, social and environmental data. There are two different application procedures, one for aggregated data and one for record level data. For the latter case, the researcher should sign a document explaining the policy for requests of record level data files

	and fill out the request for record level data form. Before person-identifiable data can be released, prior approval for the data must be obtained from the relevant authorities and the same applies to ethics approval/clearance (when applicable, as determined by the Data Controller). Website: https://deputyprimeminister.gov.mt/en/dhir
Nether-lands	In the Netherlands, Statistics Netherland (CBS) can be seen as a data access body though it has not been set-up as a data access body for health care data (see also section 7.7 for a detailed description). CBS collects individual level data from a variety of sources for its statistical output or contribution to Eurostat. The Act on CBS allows researchers to use the CBS microdata in a secure environment. This can also be done by remote access and researchers are even allowed to bring their own data, provided that they have a legal ground to process and combine the data and may combine those with CBS data including the data about causes of death. There is strict output control and only the fully anonymised data can be exported. Though there is control by CBS on the type of research being carried out, this control cannot count as ethical review of the research. CBS is an independent administrative body according to Dutch law. It is funded by Dutch government. Researchers who want to make use of the microdata pay a fee for setting up the remote access facility and additional costs of CBS for running the analyses.
Portugal	The **SPMS - Shared Services of Ministry of Health**, Portugal is a public enterprise created in 2010, with the aim to provide shared services – in the areas of purchasing and logistics, financial services, human resources, information and communications systems and technologies – to organisations operating specifically in the area of health, in order to "centralise, optimise and rationalise" the procurement of goods and services within the National Health Service (NHS). It has the status of National eHealth Agency in Portugal and manages information systems that support the daily activity of health professionals in the Portuguese NHS. At SPMS national and institutional level, a Coordination group for "Secondary use of health data" requests has been created to manage requests of health data for secondary use purposes. This group is multidisciplinary (data analysts, health professionals and legal experts) and reviews requests to be submitted to the Data Protection Officer, ensuring a single point of entry and smooth path for researchers from request to data sharing. It manages and oversees the entire process, from request to data sharing. Website: http://spms.min-saude.pt/
Slovakia	The **National Centre of Health Information (NCHI)** operates the national EHR system and certain health registries. It hosts the data and researchers can submit a request for NCHI to prepare datasets based on data in its registries (a project submission is necessary in such cases). Financing shall be required and NCHI usually will require to be co-researcher. NCHI website
[For informati on United Kingdom]	A national institute for health data in England, Wales, Scotland and Northern Ireland has been created recently, called **Health Data Research UK (HDR UK)**. It works with a wide range of health data from the NHS, universities, research institutes and charities, and increasingly from wearables, and private companies. HDR UK is a federated institute, benefiting from teams and physical offices located across the four nations of the UK. It is an independent, non-profit organisation supported by 10 funders (the British Heart Foundation, Chief Scientists Office, Health and Care Research Wales, Health & Social Care R&D Northern Ireland, Engineering and Physical Sciences Research Council, Economic and Social Research Council, Medical Research Council, National Institute for Health Research, Wellcome, and UK Research and Innovation).

	Data can be accessed via the Health Data Research Innovation Gateway. This portal provides a common entry point to discover and request access to UK health datasets. Detailed information about the datasets are made available by members of the UK Health Data Research Alliance. Before a researcher is granted access, their study is usually assessed by an independent review committee or other decision-making group, who ensure that the reason for using the data is appropriate. Website: https://www.hdruk.ac.uk/

*Please note that these examples may not cover all relevant bodies present governing the processing of health data, as some may also be related to a subset of the data (such as data from the public health system or on a specific range of diseases).

7.3. Key characteristics of data access bodies

The survey looked further into how data access bodies are organised, including their geographical coverage, their legal status, as well as how they provide access to data, the types of researchers they serve, their access models and their financial models. These issues are presented in Table 7.2 and described more fully in the sections below it, and complemented with information from the case studies. Table 7.2 is a composite of responses given to a range of questions as in Table 7.1 (see also Table A1.17-18 in Appendix 1). It also includes some information that comes from desk research and in-depth case studies rather than the correspondents.

Before discussing the data presented in Table 7.2, it is important to highlight that it does not tell the full story, as to do so in a tabular format would be very difficult. In a few cases we therefore rearranged data, which may differ from the original interpretation of the country correspondent, and in particular regarding the decision to incorporate a country as having a "centralised data access infrastructure" as that term is open to interpretation and can thus vary.[27]

Similarly, and as referred to earlier, the existence of a governance and access body does not imply that it provides *exclusive* access to personal health data for research purposes, and hence in all Member States other additional access points are also available, for example when it comes to data by different data controllers over e.g. EHR data, health insurance claims data and disease registries, as is the case in the Netherlands.

[27] E.g., UK is included in the table and the following sections even though the correspondent for the UK did not originally consider the data access system adopted in the UK, known as Health Data Research (HDR UK), to fit well into the description of a "centralised data access infrastructure", as it does not hold or store any patient or health data itself. However, it seemed appropriate to include the UK in this section as HDR UK does provide access to curated datasets of health data (including data from blood or tissue samples, images, and other personal health data) that are drawn from NHS and social care providers (including hospital and primary care administration data) as well as research institutes and charities.

Table 7.2 Key characteristics of data governance bodies ('centralised' governance bodies)

Key Characteristic	Sub-characteristic	Total MS	
Exists at national level		13	BG, DK, DE, IE, EL, FR, CY, MT, NL, PT, SI, SK, FI, [UK]
Public sector entity		13	BG, DK, DE, IE, EL, FR, CY, MT, NL, PT, SI, SK, FI
Hosts data		8	FR, BG, DK, DE, EL, NL, FI, SK, [UK]
Provides access to data stored with the original data controller		2	RO, FI, [UK]
Type of data to which access is provided	Primary care electronic health records	5	DE, MT, NL, PT, SI
	Hospital electronic health records	7	DK, DE, FR, MT, NL, PT, SI
	Social or long-term care	4	DK, DE, NL, SI
	Health insurance claims data	5	DK, DE, EL, FR, NL
	Prescribing and dispensation records	7	DK, DE, EL, FR, NL, PT, SI
	Disease registries	7	BG, DK, EL, MT, NL, PT, SI
	Bio banks	1	DK
	Genomic data bases	1	DK
	Linked health, social and environmental data	6	BG, DK, DE, MT, NL, SI
	Other	3	IE, CY, FI
Available for research for health system monitoring, management and evaluation by a public sector entity **(Function 2)**		12	BG, DK, DE, IE, EL, FR, CY, MT, NL, PT, SI, FI, [UK]
Available for research for medicines and device monitoring and evaluation (including pharmacovigilance) by public sector organisations (including regulators) **(Function 2)**		10	BG, DK, DE, IE, FR, CY, MT, NL, SI, FI, [UK]
Available for scientific research by not-for-profit and academic organisations **(Function 3)**		12	BG, DK, DE, IE, EL, FR, CY, MT, NL, PT, SI, FI, [UK]
Available for scientific research by commercial scientific organisations (**including pharmaceutical and medical technology industry) (Function 3)**		10	BG, DK, DE, FR, CY, MT, NL, PT, SI, FI, [UK]
	Possible under the same conditions as for public entities	5	BG, FR, MT, NL, FI
	Possible under different conditions	3	DK, DE, SI
Available for scientific research by any commercial organisation **(Function 3)**		4	BG, DE, SI, FI
Available for data requests from researchers in **other EU Member States**		5	DK, DE, FR, NL, FI, [UK]
Charges access fees	No	5	EL, FR, CY, MT, PT
	Yes	6	BG, DK, DE, NL, SI, FI
	Same fee for all	4	BG, DK, NL, FI
	Differentiated fees	2	DE, SI

Note. For some Member States information is missing, either as the country correspondent did not consider the body as a centralised body or the information was missing.

7.3.1. Detailed description of the components of Table 7.2

Below, we describe the various elements in more detail. It is inherently a summary of main common (or distinguishing) factors. Notably, data access systems operated in the Member States are very closely linked to the wider politics and policies of health services and health services research of each Member State, as such bodies have many variables and nuances that cannot easily be compared across countries.

Geographical coverage, legal status and data hosting or access granting

All bodies exist at national level, and most are public sector bodies. We note that in Portugal and Greece, the bodies in place (SPMS and IDIKA S.A.) are both public undertakings, but are in the table classified simply as a public entity. The majority of bodies host data, in some cases by collecting copies of already existing databases in which directly identifying personal information has been removed, as in the case of the Health Data Hub in France. Two MS (Romania, Finland) provide access to data stored with the original data controller. Of these it is worth noting that Finland provides both types of access in some cases. In most Member States the data governance and access bodies evaluate the eligibility of a request for access, take care of the processing on behalf of the requestor and anonymise data before providing them to the requestor. Note that in three Member States (Cyprus, Greece and Ireland) the answer is left open, but based on the additional information provided, Cyprus and Greece appear to host data themselves, both being national institutes of statistics or public health, while the Irish case operates as REC.

As regards the UK the body in place, Health Data Research UK, is a non-profit company limited by guarantee, owned by UK Research and Innovation, with funding from charities and public bodies. As example of a model that does not host or store any patient or health data itself, the HDR UK holds information or descriptions of the different types of datasets in the UK. It includes those held by, for example, the NHS, charities, and disease registries, this to enable researchers to see what's available and how they can access it. If a researcher wants to access a dataset, they can send a request via the HDR Innovation Gateway and the request will be considered by the organisation that looks after that dataset. Research on the data is carried out in what is termed a Trusted Research Environment or Safe Haven, these are highly secure digital spaces – physical servers in a locked room or a Safe Cloud – that can only be used by researchers who have been permitted entry. Any technology companies involved in providing or supporting the Safe Havens will not be able to see or access the data. The aim is to enable maximum security, through multiple layers, and to minimise the risk of anyone's data being misused.

Types of data to which access may be provided

Table 7.2 also shows that the data governance and access systems adopted by Member States may vary significantly from one another, not in the least because some draw on a very wide range of data, including linkage to databases outside the area of health, while others are highly focused to one type of data. The infrastructure operated in Bulgaria, for example is only for access to data from disease registries, while other Member States have data governance systems that may include a wide range of data sources. Three Member States used the category 'other' to describe the types of data that may be provided (IE, CY and FI).

Of these, Ireland is of special note, as it has created a new system, but which at present is useable for COVID-19 related issues only. With respect to Cyprus the correspondent noted that all data requests are assessed on a case by case basis, accordingly any data

could be made available if the access criteria are fulfilled; hence the category 'other' was used. Finland, having one of the most comprehensive data governance infrastructures in the EU was also marked as 'other' because it allows a requestor to be provided access in Findata's infrastructure to data obtained by Findata from any national registry data and any relevant other sources, with the exact responsibilities for both Findata and the relevant data controllers from whom data are obtained defined in Section 6 of the Finnish Act on the Secondary Use of Health and Social Data (552/2019), see also Section 7.7.

Data users and types of data use

Thirteen MS correspondents responded to questions about access to data via a central governance body in their MS. All indicated that the data made available by such a body is available for policy-making or regulatory decision-making for e.g. health systems monitoring and medicines and device monitoring by public sector bodies, as well as for scientific research by not-for-profit academic organisations. Also use of data by public bodies is mostly possible for medicines and device monitoring. Portugal did not indicate that this is the case for their central governance body, but the reason was that pharmacovigilance is managed by another body, the National Drug Agency (which also allows this data to be provided for analysis upon request). In most cases, access to data is not restricted to public actors, although there may be some differentiation in access based on the types of bodies and types of data use. Commercial actors are also able to obtain access, with most bodies differentiating between commercial scientific organisations (including pharmaceutical and medical technology industry) and other commercial actors. Conditions may apply, such as that the research should have public value, the request should be in accordance with a specific law or that additional authorisation to provide access to data to commercial actors is needed. E.g., in the German example of the Research Data Centre commercial actors cannot access the data directly. Instead, authorised users may work together with third parties and transfer anonymised and aggregated data received from the Research Data Centre to them including for research purposes with the permission of the Research Data Centre, this to enable public-private research collaborations. In the UK, the use of HDR services and the access to data will depend on the access rules applicable to the data controller of the primary data set. Portugal and Cyprus did not indicate that the data governance infrastructure can be used to gain access to data for research by commercial actors, but Portugal does allow commercial actors to access data held in disease registries for scientific research.

We also asked if commercial actors are able to use the infrastructure to access data for purposes of pharmacovigilance, medical device and medicines safety. Five correspondents indicate that this would be possible under the same conditions as for public authorities, while three indicate that different conditions would apply (Table 7.2). In Germany such private actors are not part of a list of pre-identified eligible actors, and as mentioned above and in Box 7.5, can only receive data for research with additional permission from the Research Data Centre. The private actor receives the data through the cooperation with an entitled entity. The Netherlands does not explicitly exclude commercial applicants requesting access for research purposes, but provides access to personal data for selected organisations such as universities and governmental bodies, plus the research departments of any other organisations, as long as they have been approved by Statistics Netherlands and approved research institutes that have a research department (article 41(2) of the Act on CBS). Yet, the national law does not state which criteria a research department must fulfil, and what occurs if e.g. an industry party would set a up a 'research department' that might count as research department in the sense of article 41.2 (2) of the Act on CBS. There is also no case law known where a researcher appealed a decision of CBS not granting it the status of research department.

A specific element to address is whether public authorities also have some form of priority access to personal data when requiring this for wider public health purposes, as defined in this study to fall under function 2, wider public health purposes including among others protection against serious health threats and ensuring quality and safety of healthcare and of medical products and medical devices). Table 7.2 shows that data can indeed be used for those purposes, and the implications for user fees are described below. Other than lower or no user fees, additional access criteria are often not specified and this can thus often not be answered based on applicable legislation. E.g., while the Netherlands does not explicitly differentiate on this basis in the national legislation, such differentiation is also not prohibited. Hence, it may be that such requests are still processed with higher priority, as has been the case for research in the public good regarding the COVID-19 crisis. Similarly, in Germany, there is no prioritised treatment set in the legislation for access by public bodies. Additional insight is provided in an evaluation report of the data processing by the German Institute for Medical Documentation and Information (DIMDI), as predecessor to the currently established Research Data Centre. That evaluation pointed, among others, to potentially long average processing times of applications, in part as applications from e.g. the Federal Ministry of Health with a model character and with special importance are processed with priority. A number of measures were therefore proposed, including to regulate the priority handling of applications with a model character and / or special urgency or reserve separate resources for these. It is now yet known how this will be arranged in the newly established Research Data Centre, as the practical implementation of this will depend on how the independence of the Centre will be interpreted, implemented and (may be) controlled.

Applications for access from other EU Member States

The country consultants from Denmark, Germany, France, Netherlands and Finland indicated that access is allowed by applicants from other EU Member States. For other Member States this was often not known, but none of the correspondents reported any explicit exclusion of such applications. Also based on additional clarification, it therefore appears that - in principle - all authorities allow for access by applicants from other EU Member States. In some cases (e.g. Spain) collaboration with a local partner is required, but in most cases this does not apply. Another reason for not answering 'yes' turned out to be that in a number of Member States the routes to requesting such data are less straightforward, e.g. by not yet offering an entry portal via their websites, and specifically also in other languages. Interestingly, there are also bodies such as Findata that explicitly encourage the use of data by foreign applicants to allow for internationally comparative research. Findata does make a distinction in the price of data permits between those applicants, whose place of business is in Finland or another EU or EEA country versus those whose place of business is not in an EU or EEA country (1,000 vs 3,000 EUR). Interviewees at various bodies also mention the practical barrier of then requiring a system to support the verification of a standardized way to control the identity of the foreign data applicant. E.g. in Finland currently, the identification and thus, submitting a data permit application, is only possible for persons who have a personal identity code registered in the Finnish Population Information System.

Findata is mapping alternative secure identification of applications from international (EU and other) applicants. For the future, the suggestion was therefore made to develop an identification system at the EU level, similar to what is being prepared as part of the Clinical Trials Directive, the EC Transparency Register or the Participant Identification Code (PIC) used among others for research applications.

Budgets and user fees

The research data sharing infrastructures are mostly run by a dedicated governmental agency or a public undertaking, which is governed via specific legislation. The infrastructure is usually paid for via taxes by the central government, although there may be co-payments by the users of the data. All data permit bodies listed are public bodies or undertakings that receive funding, either directly from the Ministry of Health (e.g. Finland) or from other sources such as the statutory health insurance companies for the Research Data Centre in Germany. Annual budgets can differ considerably. The Health Data Hub France is, for example, financed mainly by the public sector and was granted initial funding of 36 million euros for four years; a further 40 million euros came from the national health insurance expenditure target (L'Objectif national de dépenses d'assurance maladie, ONDAM). In comparison, Findata has an indicative budget of 1 million EUR, although the budget was higher in the years 2019-2021 to start operations.

Fees for making the data available and for using the secure data environment of the data permit authority are rather common. From the Member States for which the correspondent indicated that a fee is used, the majority also indicates that the fee is the same for all types of data users. This still allows for a differentiation of fees, but this mostly takes place based on the number of working hours required to provide the data and/or the volume and complexity of the data. Only the German and Slovenian consultants report on a differential fee structure, depending on the entity requesting the data. In the case of Germany a number of bodies are exempt from paying fees and reimbursing expenses in accordance with the provisions of the Data Transparency Fee Ordinance (DaTraGebV), this includes the statutory health insurance funds, the federal and regional associations of health insurance funds, the German Federal Association of Health Insurance Funds and the Federal Ministry of Health. In Slovenia it is noted that it may occur that public institutions are not charged for the analysis, processing and preparation of data. With regard to private companies using data for pharmacovigilance, medical device and medicines safety, Slovenia pointed to the fact that fees are differentiated, depending on the entity requesting the data - e.g. public authority, public researcher, private researcher, industry etc.

7.3.2. Data Access, including anonymisation and/or pseudonymisation

In this section we address *in what form* data can be accessed. As a starting point, Member States can differ in the labels used to mark the data held in the centralised data access infrastructure (Table 7.3). Using a pseudonym is most common, used by six Member States in total (DK, DE, FR, NL, PT, FI), though with different methods being applied (such as an algorithmic pseudonym of the patient's name or ID number or created from several factors). Four Member States use fully anonymised data, but at least one indicates that this is because the centralised body refers mostly to aggregated statistical data.

Table 7.3 With which, if any, label are the data held in the centralised data access infrastructure marked

Label of the data	Total MS	
Patient's full name	2	EL, FI
Patient's national civic number or patient ID	2	PT, FI
An algorithmic pseudonym of the patient's name	1	FI
An algorithmic pseudonym of the patient's ID number	3	DK, PT, FI
A pseudonym created from several factors	4	DE, FR, NL, FI
Fully anonymised	4	BG, MT, SI, FI
If a pseudonym is used, can it be used to link data across various data sources?		
Yes		FR, DK, DE, NL, FI
No		-

For ensuring GDPR compliant access to such data, both anonymisation and pseudonymisation tools are commonly used, partially depending on the nature of the data request. In Finland, access to pseudonymised data can be granted within the secure infrastructure of Findata, but an approved data permit is necessary, which can be applied for in Finnish, Swedish or English, via the Findata web portal. It is also possible in specific cases to obtain access within that secure infrastructure to full personal data sets in duly justified conditions, based on needs of the data applicant and processing purposes and for duly substantiated reasons. In Germany the governance body at BfARM currently only provides access to insured and service provider-related data as well as cost and administrative data, for which no permission of citizens is needed (see also Box 7.5 – section 'data altruism' for a description of relevant changes). In principle, researchers obtain anonymised data, unless pseudonymised data are necessary and there is no other means of obtaining the data. In the case of pseudonymisation, the risk of re-identification is assessed before the data are provided.[28] Risks are then minimized while adequately safeguarding the intended scientific benefit through appropriate measures. In the Netherlands, linking of data takes place within the Statistics Netherlands environment. Researchers can bring their own datasets which will then be linked with the data of Statistics Netherlands. Researchers can only export the statistical output, which is checked beforehand upon non-identifiability. As last example, the French correspondent indicates that a pseudonym is used for data that is made available to actors, accessing one or more of the repositories being a component of the SNDS (Système National des Données de Santé) for research, study or evaluation purposes.[29] Only the central management body of SNDS has the key. Any linkage between databases is always done outside the Health Data Hub by a national trusted third party. For this, it is necessary to anticipate that two databases will have to be linked and to ask the third party to

[28] In some cases pseudonymisation is also used so that where a real and specific health danger is identified for an individual they can be contacted in line with the ethical principle of incidental findings (see also section 8.2.1 on anonymisation and pseudonymisation).

[29] This applies to the following databases: SNIIRAM [health insurance data], PMSI [hospital data], CepiDC [Medical causes of death]).

generate identical IDs for these two databases. A pseudonym code is generated for each individual for all the data concerning him/her in a given project space. The IDs are not the same between project spaces.

7.4. Data altruism

The discussion above has focused on re-use of data from sources such as EHRs, hospital information systems and disease registries. These are well established sources of health data for research, and ethical codes have been adopted in many Member States to ensure that they may be used for research purposes. However, as personal health records, personal health spaces and the use of personal health and wellness devices and apps is increasing, the concept of **data altruism** becomes relevant, in addition to the existing mechanisms for further use of patient data for research based on notions of public health and solidarity.

7.4.1. What the literature says

In the Communication on the European Data Strategy, the European Commission outlines the concept of fostering data altruism, through which individuals can make data concerning themselves available to researchers for public good purposes (COM, 2020a). In addition to data altruism, the term 'data solidarity' might also be suitable, since in the area of health the ultimate objective is to generate knowledge resulting in better health care from which future patients will profit. Data altruism, or the possibility of making personal data available for research may be regarded as key to better and more health data use, especially in Member States where - in relation to the provision of health data - the rights of individuals rather than public interest prevails.

Notably, both the terms data altruism or data solidarity have been used in preference to the term data donation as the latter implies ownership transfer - one cannot give away fundamental rights on his or her personal data. Furthermore, the concept of ownership does not fit comfortably with health-related data in all situations. A healthcare record is not only a record of data concerning a patient, it is also a record of the professional interventions as well as a reflection of the opinions of the healthcare professionals who interact with the patient. In some situations the record may also contain information about others in the patient's circle, such as family and carers. Furthermore the medical history of a patient necessarily implies information about antecedents and descendants, many of whom may still be alive; and finally as we move to more personalised medicine and the inclusion of genetic information, the links to other individuals both living and dead becomes clearer. Many academic articles have been written on this issue, amongst which a compelling argument is made by Ballantyne (2020) who argues that "clinical data are co-constructed, so a property account would fail to confer exclusive rights to the patient. A non-property account of ownership acknowledges that the data are 'about the patient', and therefore the patient has relevant interests, without jumping to the conclusion that the data 'belongs to the patient"; she goes on to note the concept of ownership could even be harmful to the promotion of notions of data altruism, as ownership (and therefore the passing of ownership to another) risks severing of the connection between the patient and their data, and missing the opportunity of engaging patients in the data research enterprise.

In support to the notion of data altruism several studies show that the general (European) public generally is supportive to reusing health data, as long as a number of criteria are met, such as the trustworthiness of those who are able to access the data, the perceived sensitivity of the data and the degree to which the data are expected to contribute to the public good (Skovgaard et al 2019; Karampela et al 2019; Shah et al

2019; Stockdale et al 2019). Studies have also shown that significant concern exists when data are used by commercial entities. A survey among rare disease patients (who are often thought to be best informed patients and most inclined to become involved in research) indicated that while they have high confidence in academic and not-for-profit organisations re-using data for research, they are less confident when data are used for research by governmental or commercial organisations (Courbier et al 2019; see also Castell & Evans 2016). Karampela et al (2019) and Stockdale et al (2019) mention that an opt-in model of consent is valued as a more trusted data sharing practice. Yet other studies show that opt-out is also acceptable if certain conditions are met (Skovgaard et al 2019). All studies show the importance of awareness and transparency of safeguards being in place. Trust issues are also centred around an organisation's ability to ensure data security and the motivations of the organisation to store and collect data.

7.4.2. What is taking place in Member States?

The country correspondents reported that only two Member States are currently preparing some form of data altruism or data solidarity system (Germany and Denmark, both being clarified in greater detail in case studies in section 7.7). The correspondent for Denmark mentions Sundhed.dk and their strategy for the coming two years through which they wish to open up safe spaces for storage of citizen generated data which could be marked as available for research, but this is not operating yet. Germany also does not yet have a data altruism model based on the patients' consent in operation, but this is being implemented with the Patient Data Protection Act, providing insured persons as of 2023 the option of making data stored in the electronic patient record available for research. It is worth also noting that the UK has a data altruism or data solidarity system in place; details on the UK case are added in Box 7.2.

It is worth noting, however, that some Member States have systems in place that could be viewed as a form of data altruism, but perhaps not the full concept of data altruism as foreseen in the recently published Draft Data Governance Act, which notes in recital 38 that "data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7" of the GDPR (COM, 2020b). A typical example in such first steps towards data altruism is when disease registries are made available for certain types of research. In Ireland, for example, access to data in the National Cancer Registry may be provided by the data controller to some researchers. This system demands notification of patients, a high level of transparency and the right to refuse or withdraw. While this is not data altruism as foreseen in the Data Governance Act, which places a high level of emphasis on consent, it remains an important tool for ensuring that certain health data that is crucial to advancing scientific research may be made available to researchers in an ethical manner. In overview, Member States are exploring possible options for translating the concept in existing infrastructures, such as by enabling an interactive and dynamic consent option through the electronic health records system. It remains to be seen whether such systems are functional on the longer run and will not lead to consent fatigue or selection bias which would make research based on those data unreliable. Next to Member States initiatives, also bottom-up initiatives exist, often called *data cooperatives* in which citizens can share personal data for research purposes. When organised as citizen-owned non-profit cooperatives, these are argued to provide a basis for more democratically controlled and fair personal data ecosystems in which citizens are empowered to become active participants in science (Hafen 2019). Current examples include various initiatives, such as MiData and HealthBank, both in Switzerland and Salus Co-op in Spain, or the (public-private partnership) National Experimental Therapeutic

Partnership (NEXT) in Denmark, a database in which patients can register to make them easy to find and enrol into clinical trials if they wish to participate.

Table 7.4 Data altruism in place or desirable to set up at national or EU level

Is a system for data altruism in place?	Total MS	
Yes in place, or in process of being implemented	2	DK, DE, [UK]
No	25	BE, BG, CZ, EE, IE, EL, ES, FR, HR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, SK, FI, SE
If no, do you believe that a system of data altruism should be set up at national level?		
Yes	14	BG, CZ, EE, IE, EL, ES, HR, CY, LV, MT, NL, RO, SK, FI
No	1	SI
Not sure	10	BE, DK, FR, IT, LT, LU, HU, AT, PL, PT
Do you believe that a system of data altruism should be set up at EU level?		
Yes	11	BE, BG, CZ, DE, EE, EL, LV, LT, HU, SK, FI
No	5	ES, IT, CY, NL, SI, [UK]
Not sure	11	DK, IE, FR, HR, LU, MT, AT, PL, PT, RO, SE

* To illustrate the responses, EE answered both yes and no, with the clarification that the answer in the current settings would be 'no', and to be changed to 'yes' if first clear regulations with responsibilities were set in place.

Box 7.2 Opt-out of the data altruism system in the UK

In England, the "National data opt-out" was introduced on 25 May 2018, which is an NHS England/NHS Digital policy initiative enabling patients to opt out from the use of their data for research or planning purposes. Confidential NHS patient information might also be used to plan and improve health and care services and to research and develop cures for serious illnesses. It is used by the NHS, local authorities, university and hospital researchers, medical colleges and pharmaceutical companies researching new treatments. National data opt-outs apply to a disclosure when an organisation, for example a research body, confirms they have approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by another organisation responsible for the data (the data controller) such as an NHS Trust. The CAG approval is also known as a section 251 approval and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002. The NHS Act 2006 and the Regulations enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed without the data controller being in breach of the common law duty of confidentiality. In practice, this means that the organisation responsible for the information (the data controller) can, if they wish, disclose the information to the data applicant, for example a research body, without being in breach of the common law duty of confidentiality. To be clear - it is only in these cases where opt-outs apply.

The national data opt-out does not apply:

- Where explicit consent has been obtained from the patient for the specific purpose.
- Where NHS Digital indicate data should be provided to them (NHS Digital) under s259 of the Health and Social Care Act 2012.
- To the disclosure of confidential patient information required for the monitoring and control of communicable disease and other risks to public health. This includes any data disclosed where Regulation 3 of The Health Service (Control of Patient Information) Regulations 2002

provides the lawful basis for the common law duty of confidentiality to be lifted.

- Public Health England oversees the use of this legal gateway on behalf of the Secretary of State for Health and Social Care.
- To the disclosure of confidential patient information where there is an overriding public interest in the disclosure, i.e. the public interest in disclosing the data overrides the public interest in maintaining confidentiality. This should be as a result of a positive public interest test having regard to the circumstances of the case. Data controllers are expected to have their own arrangements in place to apply the public interest test as and when necessary.
- To the disclosure of confidential patient information where the information is required by law or a court order.

All NHS organisations must provide information on the type of data they collect and how it is used. Data release registers are published by NHS Digital and Public Health England, showing records of the data they have shared with other organisations.

Scotland has a separate opt-out, offered through the Scottish Primary Care Information Resource (Spire) (https://spire.scot/).

Also, the Scottish Health Research Register (SHARE) is a NHS Research Scotland initiative created to establish a register of people, aged 11 and over, interested in participating in health research and who agree to allow SHARE to use the coded data in their various NHS computer records to check whether they might be suitable for health research studies. This means that they are not donating their health data per se, but making their contact details available for researchers to contact them to ask them whether they wish to participate in a research project (by providing their consent). To date, over 281,000 people and Scotland have registered for SHARE (out of a population of 5.5 million)."

7.4.3. What the future may bring

Despite the fact that only two Member States have a system to support data altruism on a national level in process of being implemented, the concept would seem to be well accepted with correspondents from fourteen countries indicating that they consider this as desirable. Ten were not sure and one rejected the idea of setting up such a system. Country correspondents also suggested various options for the creation of a system of data altruism and identified possible challenges, including the need for clear information to the public in order to create awareness, understanding and willingness with regard to data donation. Such information would also need to develop a common understanding of the concept of 'data altruism'. Furthermore, the issue of potential gain of commercial organisations needs to be addressed, as resistance to data solidarity may arise if people have the feeling that commercial parties gain profits with the data they donated. The need for unification of rules concerning topics such as the legal bases, collection of data, storage, access, and security measures was also highlighted.

The need to build trust in any system adopted was stressed, and it was noted that this could be supported by providing feedback on research results to data subjects and the public at large. Trust building could also be enhanced by having an opt-out option from data sharing, as already implemented in some countries for certain types of data sharing. Belgium, for example, has an opt-out system for tissue research, and France also has an opt-out system for collecting personal health data in registries. In the UK the opt-out system is more nuanced, with in general data research using opt-out but tissue research using opt-in (see Box 7.2 for more details). For countries with decentralised healthcare systems it is a challenge to assess at what level (national or decentralised) rules and data infrastructures should be defined (as in Spain).

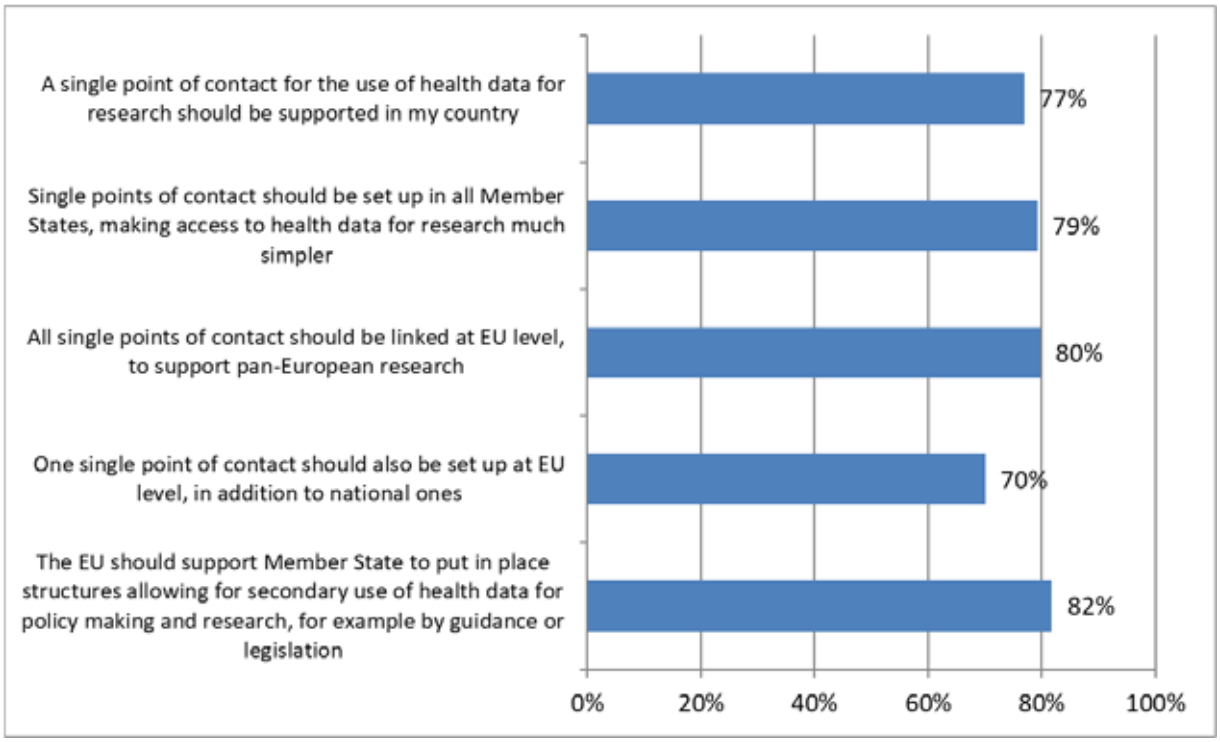
A framework can be either national, as some correspondents suggest, or could be set up as network of local or regional or sectoral of public or private databases with guidance on ministerial level.

Looking at the idea of an EU level system for data altruism, eleven correspondents believed such an EU system should be set up; eleven were not sure and six did not think this is an EU task. As part of the extra clarifications to this question several correspondents noted that such an EU level system should be voluntary, and that an EU level public body to promote data altruism could be helpful. One country correspondent voiced doubts as to the feasibility of a specific EU level data altruism system, since it would be costly and not as comprehensive as the information in the EHR records of healthcare providers.

7.5. Stakeholders views

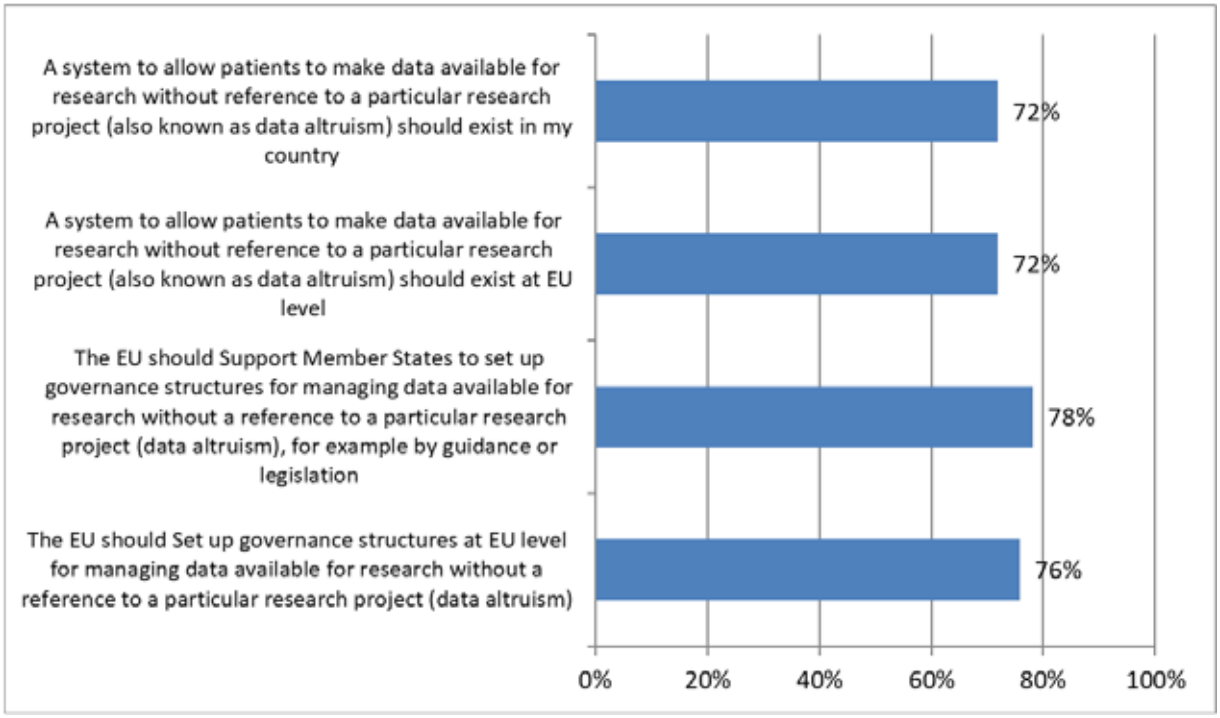
The results of the stakeholders survey point in the direction that the EU should support Member States to put in place a structure allowing for secondary use of health data; this can be done by a single point of access, though legislation or by guidance, according to the stakeholders. Single points of access are considered to facilitate research trough easier access and to be supportive to pan-European research. The stakeholders also express a preference for a single point of contact at EU level (Figure 7.2).

Figure 7.2 Share of stakeholders agreeing with the following statements, all related to whether data sharing for scientific research could be improved



The stakeholder survey also showed a high level of support for the concept of an EU level system for data altruism, although almost three quarter of the survey's respondents thought that it should exist in their Member State as well as at EU level. Many also thought that the EU should support Member States to set up these structures and set up such a structure at EU level (Figure 7.3).

Figure 7.3 Share of stakeholders agreeing with the following statements, all related to whether data altruism for scientific research could be improved



7.6. Concluding remarks

In this chapter we described that national governance models, strategies and governance frameworks for access to health data for secondary purposes can differ considerably between Member States, in part also along the lines of the types of data sources used (electronic health records, registries, around other infrastructures and database). In some Member States there is one or a limited number of national agencies or bodies authorised to grant permits for the re-use of data already collected, while in other Member States the landscape is far more decentralised, with a wide range of bodies managing the access to health data for research and public policy purposes.

The diversity both within and between Member States indicates that developing potential synergies of such governance frameworks to move towards an EU level health related data governance infrastructure will be a complex task. However, the concept of such a strategy has been endorsed through the commitment to a European Health Data Space in the European Commission's Data Strategy (2020b). While the details of the infrastructure and governance are still being developed, it is worth noting that the Digital Gateway Regulation (EU 2018/1724) already promotes the principle of recording data only once and promoting re-use of data where possible. The focus of the Regulation is on making government use of data more effective, simpler and to reduce administrative burdens for citizens and businesses by re-using data within government. The principle requires public administrations to "ensure that citizens and businesses supply the same information only once […]public administrations should take action, if permitted, to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses"[30]. The discussion in this chapter, and indeed the report, indicated that

[30] The once-only principle is among the seven underlying principles of this action plan to make government more effective, simpler and reduce administrative burdens for citizens and businesses by re-using data within government. The principle requires public administrations to "ensure that citizens and businesses supply the

such a balance would be complex to achieve with respect to health-related data and would demand a high level of commitment from the Member States, but the concept of once only by recording data once could serve as concept for the development of an EU level health data governance model.

7.7. Within-chapter annex: detailed description of case studies

The information presented in the previous sections was partially based on a set of in-depth case studies, conducted on a selection amongst the 13 Member States who have a centralised governance and access body present, in order to provide more insight on the variation in forms of such bodies. For easier reference, we present the six case studies as part of this chapter rather than as a stand-alone annex at the end of this report.

To clarify the selection of case studies, in the course of the project a clustering of Member States was identified based on the horizontal mapping of the governance and access bodies put in place by MS, with governance in some Member States being arranged in more centralised formats while other Member States rely more on within-sector and decentralised approaches.

- Three cases are highlighted to describe a more centralised approach, having a national public agency or public undertaking authorised to grant permits for the use of data already collected for a specific purpose (being Finland, Germany and France).
- Other countries encompass a more decentralised approach for the governance of data sharing, often as they see fitting with their national contexts. Highlighted cases include Denmark, Spain and the Netherlands.

We should note that this distinction is not clear-cut and that hybrid forms exist. Given that the case studies are relatively diverse, they can also not be compared on exactly the same criteria. E.g. in the case of national level bodies, there is a logic in mapping the budget, sources of funding and operations (to the extent that this information is made available), but for more decentralised contexts, with governance bodies e.g. in different regions or covering a broad range of bodies, data on such quantifiable measures are reported where possible, but may be fragmented and not be comparable across other Member States.

Box 7.3	**Findata, Finland**
Description	Findata is the brand new Finnish Data Permit Authority, acting as 'one-stop-shop' for health and social data access, in operation since January 2020 (www.findata.fi). The services Findata provides are to 1) grant data permits to data from multiple registers; 2) collect the requested data from the controllers and then combining, pseudonymising and anonymising the data or producing statistical data, and 3) deliver the data for use to the requestor for use in a secure remote IT environment, potentially also by converting and combining the permit holder's own data.
Background	Findata was set up with the goal to enable fast, easy and safe access to health and social personal data. Before, one had to request access to all data controllers separately, which was a very time-consuming and administrative process. On top of that, data was not processed in a secure and controlled way.

same information only once […]. Public administration offices take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses"

	Findata started operating in steps. Since January 2020, data requests for statistical data can be made. Since April 2020, data permit applications can be issued. From January 2021, Kanta services, where medical records are stored, will be included. Up to 12 October 2020, a total of 230 data applications were received, of which 143 data permits for personal data and 35 data requests for statistical data.
Legislation	The Act on the Secondary Use of Health and Social Data (552/2019) specifies the purposes for which one can request data access. It applies to register based research, and not to clinical trial data. Genome and biobank legislation are on its way. The Act among others also specifies that personal data can be used for the following purposes, even if the data was not collected for that purpose: 1) statistics, 2) scientific research, 3) development and innovation activities*, 4) education, 5) knowledge management, 6) steering and supervision of social and health care by authorities, and 7) planning and reporting duty of an authority. Further details of the implications of the act on services provided are described below. ** From this list of purposes, the purpose of 'development and innovation' only allows for the use of statistical data.*
Tasks and activities	Findata is a completely new system but builds on a long history of registries and a digitalised society. The main tasks relate to the three services described above. Findata offers services for those needing data (customers) and for those controlling data (controllers), all relate to the secondary use of health and social data. To make a data request for personal rather than statistical data, it is possible since April 2020 to apply for a data permit to access pseudonymised personal data for all above mentioned purposes, including e.g. function 2 purposes of authorities' planning and reporting duties. Only exception is the purpose of 'development and innovation', which only allows for the use of statistical data. Findata serves users of data by compiling a dataset and providing access to a secure environment to process the data. Findata cooperates with data controllers to standardize data descriptions. It also provides an anonymisation service and a permit processing service if the controller authorises Findata to do so. The Act also describes the responsibilities and tasks of both Findata, as Data Permit Authority, plus a predefined set of authorities and organisations, for the secondary use of data in the registers (being eleven different authorities and organisations such as the Ministry of Social Affairs and Health, the National Institute for Health and Welfare (THL), the Finnish Medicines Agency (Fimea) and public service organisers of health and social care) regarding the following elements: a) Data set descriptions b) Advisory service c) Collection, combination and pre-processing service for data d) Identifier administration service e) Data request management system f) Secure hosting service The Act also demands the IT-systems used for secondary use of social and health data to be audited against Findata's regulations by a Data Security Assessment Body. Findata is currently preparing to give regulations on the requirements for secure IT-environment for using and managing data for secondary use.
Governance	Findata is an independent central agency which falls under the responsibility of the Finnish Institute of Health and Welfare (THL). A steering group, consisting of representatives from data controllers whose data Findata provides access to, develops and guides Findata's operations. The Data Protection Ombudsman, Parliamentary Ombudsman and Valvira[1] supervise the operations of Findata and compliance with the Secondary Use Act. [1] Valvira is a national agency operating under the Ministry of Social Affairs and Health, charged with, amongst others, the supervision of the social and health care.
Organisation and budget	The budget of Findata is set by the temporary steering group who was preparing the implementation of the Act on the Secondary use of Health and

	Social Data. After a start-up budget in the beginning years 2019-2021, the annual budget is about 1 million euros per year, with the main expense items being personnel costs and ICT-systems. Since it is a new system, there is no data yet about the real yearly costs and gains of running Findata, but it is anticipated that the set budget will not be sufficient, and may be raised to over 2 million annually.
Staff and functions	There are currently 15 staff working for Findata, and recruitments are going on. It is expected that in a few years 20-25 staff will be employed. Functions of the staff are in the field of ICT, communications, law (DPO), metadata and data services.
Data sources and types of data	Via Findata social and health data can be accessed from various public institutions, private institutions and registries. The sources of data for which Findata can issue permits are specified in the Secondary Use Act. Findata grants permissions for data collected both in public and private sector services which are part of the relevant data sources. According to Finnish legislation, only an official authority can grant permission to use Finnish citizen's personal data. Therefore, even if the data is collected at private doctor's surgery, the private health clinic does not have the power to grant permits for secondary use. Data granted by Findata can be combined with data from other countries, and this can be done in two directions: it is possible to transfer Finnish data to secure environments in other countries, and it is possible to import data from other countries to Finland, either to Findata remote access system or to a secure audited environment maintained by some other organisation. Both forms have already been applied in several cases. Data can only be taken out of the remote access environment and disclosed to another secure user environment in exceptional cases. However, this is sometimes necessary due to restrictions from other remote access environments when data needs to be combined.
Foreign data users	In Finland currently, the submission of a data permit application is possible for persons who have a personal identity code registered in the Finnish Population Information System. Findata is mapping alternative secure identification applications for its international users. Hence, in the future, it should also be possible for foreign stakeholders to request a data permit, however, there is not yet a standardized way to control the identity of the foreign applicant. When applying is possible, there will be no additional protective restrictions for non-Finnish data users (such as having a Finnish research partner). Processing data in the remote access environment of Findata when being in a third country (outside the EU/EEA) is possible if there are appropriate safeguards in accordance with Chapter V of the GDPR. Non-EU stakeholders applying require more paperwork and possibly (EU standard) agreements, and the fee is higher.
User fees	The price of Findata services are defined in the Valtion maksuperustelaki (State Basis of Payment Act) and detailed in the Decree of the Ministry of Social Affairs and Health Fees for the services of the Social and Health Information Licensing Authority of 30 December 2019. For its public services, a processing fee is charged that must correspond to the amount of the total cost to the state of producing the performance (*cost value*). The fee (of 115 EUR per working hour) is determined based on the hours worked to produce the output (by means of data aggregation, pre-processing, pseudonymisation and anonymisation). The fee may be below the cost value of the service or may not be charged at all if there are justified reasons related to health and medical care, other social purposes, the administration of justice, environmental protection, educational activities or general cultural activities. In the above mentioned decree, a fixed fee based on the average cost value applies for the following services: • A data permit for a permit applicant established in Finland or another EU or EEA country of 1,000 EUR; • A data permit for an applicant established in a non-EU or non-EEA country of 3,000 EUR,

	• a change of data permit for a permit applicant 350 EUR. • a decision concerning a data request with a fee of 1,000 EUR. • A data permit related to a thesis and a decision on the information request for an applicant who is domiciled in Finland or another EU or EEA country of 500 EUR.[31] In addition, Findata provides remote access environment services, which are commercially priced services subject to a fee (VAT +24%). Such packages can range from a Small Package (8 GB) of 2,250 EUR/year to an XL Package (90 GB) of 8,500 EUR/year.
Pseudony-misation / anonymisation	One can access statistical level data via a data request and individual level data via a data permit. In principle, individual level data is available in a pseudonymised or anonymous format, dependent on what is requested. Access to data with direct identifiers is not excluded, but only granted under strict conditions and fitting with the data applicant's processing purposes.

** Sources of information: findata.fi, legal technical survey by national country correspondent, and correspondence with relevant experts.*

Box 7.4	**Health Data Hub (HDH), France**
Description	The Health Data Hub (HDH) is a unique gateway to health data in France. The HDH's vision is to ensure a simple, unified, transparent and secure access to health data for public interest research with the goal to improve the quality of care and patient support. The HDH is a platform where pseudonymised health data from different sources is duplicated and made available. It is both an infrastructure and a health database catalogue, and offers related services, allowing project coordinators to access data and/or link different databases. The role of the HDH is to give access to health data, promote the collection and consolidation of data, to accompany data exploitation, to support the research community and to ensure the link with civil society. The aim of the HDH is to federate all health data stakeholders, and to facilitate access to various data sources (public/private) while ensuring high standards of transparency and privacy.
Background	The origin of the HDH stems from a report written in 2018 'For a meaningful AI', where deputy and Fields Medal mathematician Cédric Villani recommended a single point of entry to access health data, as health was defined to be a key strategic sector for the development of AI in France. Following the report, President Macron announced the creation of the HDH. An in-depth study mapped the obstacles in the secondary use of health data in France, which resulted in a roadmap 'code of conduct' for the HDH. The HDH aims to become the single entry point to French health data. This system is being implemented to harmonize health data access in France and to address quality and interoperability issues of the various databases are a key part of the HDH governance model.

[31] The price related to the thesis is applied if the application concerns a research project that produces one thesis. If the application concerns a project that produces more than one thesis or a project that produces one or more theses and other outputs, a normal data request decision or data permit fee (EUR 1,000.00) will be charged.

Legislation	The Law of July 24th 2019 on the Organisation and Transformation of the Health System is the main legislative text which sets up the HDH as a public interest group (GIP) to be the main gateway to operate public interest research on the National Health Data System (SNDS). The scope of the latter has been increased by that same law to all health data fully and partially reimbursed by national solidarity. In addition, the HDH hosts an independent Ethical and Scientific Committee for Research, Studies and Evaluations (CESREES).
Tasks and activities	The missions of the HDH can be summarized in four main areas: - Supporting data controllers in the collection, consolidation and development of their assets; - Offering all project coordinators simplified and fast access to health data; - Guaranteeing transparency towards civil society and ensuring respect for citizens' rights; - Innovating alongside research and industry players.
Governance	The HDH takes the legal form of a public interest group (GIP) governed by public law. The HDH takes over the missions of its predecessor, the National Institute for Health Data (INDS) as the single entry point for health data access in France. It is also responsible for health data access governance as it hosts the secretariat of the CESREES, the ethical and scientific committee for health research, studies and evaluations, which evaluates requests for access to the data catalogue. The missions of the HDH are determined through article L. 1462-1 of the Public Health Code. The health data platform, with its governance set up by decree, is composed of 56 entities that represent the State, organisations ensuring representation of patients and users of the health system, producers of health data, public and private users of health data, including health research organisations, among others.
Organisation and budget	The HDH is a single point of entry data governance model, providing access for all researchers to data currently stored in the HDH (and SNDS). The data remains stored with the original data controller. The Health Data Hub is a central body, but does not incorporate all data. For example, biobanks and registries have their own systems. The project results are made public on the website of the HDH, with due respect for academic and industrial competitiveness. As for budget, the HDH is currently funded by the public sector. Before the official creation of the public interest group, the Health Data Hub project was conducted under the direction of the Ministry of Solidarity and Health (Directorate of Research, Studies, Evaluation and Statistics (DREES)) and was selected in the Big Data and Artificial Intelligence call for projects of the Fund for the Transformation of Public Action (FTAP). In this context, it was granted initial funding of 36 million euros for four years. A further 40 million euros came from the national health insurance expenditure target (L'Objectif national de dépenses d'assurance maladie, ONDAM).
Staff and functions	As of end of 2020, around 50 people are working for the Health Data Hub. The Hub is planned to grow further.
Data sources and types of data	The HDH can provide access to any pseudonymised health data that is reimbursed partially or fully by national public solidarity in France. This includes the national claims database, as well as in the future numerous other databases to be included in its catalogue, such as cohorts, clinical data, genomics data etc.

Data users	Data access is only allowed for public interest research, with a strictly defined project duration and a limited scope upon approval by the Scientific and Ethics Committee (CESREES) and the national DPA (CNIL). Data is accessible via a customized secure project space, containing only the needed dataset and offering a variety of data analytics tools. The data processor cannot directly retrieve data from the platform. Any private actor requesting access to the data will have to prove that the project is of public interest, for the benefit of citizens, in the same way as public actors.
Foreign data users	Data access can be granted to data users from other EU countries. The HDH contributes to the dissemination of international standards and best practices as well as to improve interoperability, in order to enable quality data aggregation and linkage. The HDH is actively looking to encourage cross-border research collaborations on health data, primarily with research structures and data controllers.
User fees	In the future, the HDH could charge fees for access to its services such as the use of the secure project space for for-profit actors. As the Hub is in its start-up phases the exact rates are still under development.
Pseudony-misation / anonymisation	The HDH only stores pseudonymised data and citizens have a right to opt out of the secondary use of their health data through the HDH. Citizens cannot object to uses made compulsory by law, or necessary to carry out a mission of public interest, for example for health monitoring purposes.

** Sources of information: health-data-hub.fr, legal technical survey by national country correspondent, and correspondence with relevant experts.*

Box 7.5	Research Data Centre at the BfArM (Federal Institute for Drugs and Medical Devices), Germany
Description	The Centre serves as a research data hub for claims data of all statutory insured people in Germany (currently covering approx. 90% of the German population). It is currently being reorganised, expanding its range of data and services. Within the next few years it will also serve as a research hub for EHR data for which patients have granted access to for research purposes.
Background	The Centre was originally based at the German Institute for Medical Documentation and Information (DIMDI), responsible for medical information classification and management. To strengthen its role, the institute was brought together with the Federal Institute for Drugs and Medical Devices (BfArM) in May, 2020 to form one authority.
Legislation	The main legislation describing the mandate of the Research Data Centre at BfArM are the §§303a-f of the Social Code Book 5 (Sozialgesetzbuch, SGB V, Statutory Health Insurance; https://www.sozialgesetzbuch-sgb.de/sgbv/303a.html). It has been updated with the Digital Care Act in December 2019 to accommodate the new role, and the Patient Data Protection Act in July 2020 to, as of 2023, also include EHR data on a voluntary basis. Based on the new §§303a-f of the Social Code Book 5 the Data Transparency Ordinance (DaTraV) (http://www.gesetze-im-internet.de/datrav_2020/) was revised in 2020. It describes the tasks of the Research Data Centre at BfArM in more detail.
Tasks and activities	As described in § 303d SGB V the Research Data Centre is tasked to handle data that is transmitted to it by the German Federal Association of Health Insurance Funds (GKV-SV) and to promote the scientific secondary use of the data for specified research and public health purposes. It, among others, includes carrying out quality assurance of the data, examining requests for data use and making it available to authorised users while balancing re-identification risks and intended scientific benefits. As separate entity, the Robert Koch Institute (RKI) performs the duties of a trust agent managing a two-layered pseudonymisation process to ensure that the pseudonymised

	claims data provided by the GKV-SV are correctly linked to the longitudinal data at the Research Data Centre. The data used for assigning the respective cross-period insured person pseudonyms to the transmission work numbers are deleted; only the algorithms are kept.
Governance	The legal supervision of both the Research Data Centre and the trusted agent has been assigned to the Federal Ministry of Health (BMG), but each maintain an operational independence.
Organisation	The Research Data Centre is based at the Federal Institute for Drugs and Medical Devices (BfArM) with an independent IT infrastructure. A dedicated trust agent unit is based at the Robert Koch Institute (RKI). The statutory health insurance companies reimburse the Federal Institute for Drugs and Medical Devices and the Robert Koch Institute for the costs of performing the task of data transparency.
Staff and functions	The staff of the Data Research Centre is currently being extended to accommodate the new duties. Within the next few years it is expected that the staff will expand to about 15 full time staff members comprised mostly of IT specialists, data engineers and data scientists.
Data sources and types of data	As defined in the DaTraV, the research centre receives pseudonymised claims data from the statutory health insurance companies for each calendar year (reporting year) per statutory insured person (covering approx. 90% of the German population). It will include among others diagnoses, prescriptions and treatment data from medical care, including in- and outpatient care, dentistry, aids and remedies.
Data users	As defined in § 303e SGB V a pre-defined list of authorised institutions can request permission to access data, and no further distinction is made between applicants. These for example include health reporting institutions at the federal and state levels, health insurance providers, relevant umbrella organisations of service providers or patients at federal level, and universities as well as university hospitals recognized under state law. This also includes publicly funded non-university research institutions and other independent research institutions, provided the data serves independent scientific projects. Commercial research institutes and industrial companies can thus not request permission for data access. Authorized users may work together with third parties and transfer query results, i.e. anonymised and aggregated data received from the Research Data Centre, to further project partners only with prior permission of the Research Data Centre. This will facilitate research collaboration undertaken between the public and the private sector.
Foreign data users	§ 303e SGB V does not explicitly list researchers or institutions from other Member States as authorised users, but also does not restrict research institutes to domestic institutions. In principle these can also be based in other Member States, as long as the data are used for scientific research, and applicable law is respected.
User fees	User fees are defined in the Data Transparency Fee Ordinance (DaTraGebV; http://www.gesetze-im-internet.de/datragebv/). Underlying principle is that the fees are determined based on the amount and complexity of the data rather than the time spent on the applications. The fee for standardized data queries amounts to 300 euros. To provide data by means of a query pre-formulated by the authorized user, the fee amounts to an additional 300 euros per evaluated year. In addition, a fee of 50 to 1,600 euros will be charged for each consultation, each preparation of preliminary evaluations and for interim results depending on the scope and complexity of the request and the associated use of personnel and material benefits. For the provision of pseudonymised individual data records in future secure, physical or virtual surroundings of the centre, an additional fee of 100 to 3,000 euros is charged, again depending on the scope and complexity of the request and the associated use of personnel and material services calculated.
Data altruism	Currently, data include claims data of all statutory insured citizens without requiring their permission. As part of the "Patient Data Protection Act" (Patientendaten-Schutz-Gesetz, PDSG) in 2020, patients can voluntarily make use of an electronic patient record (elektronische Patientenakte, ePA). From 2023 onwards, insured persons will have the option of voluntarily making the

	data stored in the ePA available to research via the Research Data Centre (source: BMG 2020)[32]. This has also been adjusted in § 363 IV SGB V: Insured persons can voluntarily release the data in their ePA for the research purposes listed in § 303e II Nos. 2, 4, 5 and 7 SGB V to the Research Data Centre. Insured persons may also make the data in their ePA available for a specific research project or for specific areas of scientific research on the sole basis of informed consent.
Pseudony-misation / anonymisation	The Research Data Centre shall provide authorised users with data that is anonymised and aggregated to the extent required for the specific research question.

** Sources of information: legal technical survey by national country consultant, legal texts as mentioned in the box and correspondence with relevant experts.*

Box 7.6	**Statistics Netherlands (CBS)**
Description	Statistics Netherlands (CBS) is the independent national statistics agency, providing statistical information on social issues, including health. Within CBS, the microdata services department was set up to allow researchers to obtain health and other data for research purposes.
Background	CBS is the central agency to access data for research and other types of secondary use of health and administrative data. However, access to health data is very fragmented in the Netherlands and there are also many other access points (e.g. regional biobanks). CBS was established in 1899 in response to the need for reliable and independent statistical information on social issues. The CBS statistics should support the public debate and policy-making and reduce social inequality by collecting, processing and publishing statistical data. CBS microdata services provides access to (linked) data for third parties for research purposes.
Legislation	The Statistics Netherlands Act forms the legal basis for CBS and precludes that any data recorded and collected in the Netherlands with public funding, may be used by CBS for their statistical tasks. Permission is needed from some of the data sources for secondary use by other parties.
Organisation and budget	CBS is an autonomous administrative authority which is financed by the state. Standard fees apply for anyone using the data. Fees are based on the number of datasets to be linked, a monthly access fee for each user, and the size of the dataset.
Data sources	The Healthcare Market Regulation Act requires health care providers to submit pseudonymised data about treatment codes to the Healthcare Authority (HCA). The HCA further processes the data and sends statistics to the Department of Health and CBS. Only treatment codes which are based on a fee for service (instead of a lump sum based on the number of enrolled patients) are sent regularly to the HCA. Health care providers are also obliged to submit pseudonymised data about treatments etc. to CBS. However, this obligation is balanced against the administrative burden of submitting data. If CBS can derive sufficient information from a representative sample of health care providers, it will not require all similar health care providers to provide data. Types of data that can be accessed through CBS are: electronic health records, both from primary care and hospitals, social care data, long-term care data, health insurance claims data, prescribing and dispensation records, disease registries, health data linked with social and environmental data. Such data can be from private or public sources. For some sources of data, separate permission has to be obtained from data sources (e.g. extracts from hospital and primary care electronic health records, claims data from health insurers). For other data sources permission

[32] https://www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html

	from CBS suffices (e.g. socioeconomic data).
Data users	Authorised institutes can use microdata sets of CBS for research purposes, which consist of linkable data sets at individual level. Authorised organisations are Dutch universities, scientific research institutes, policy advice and analysis organisations, statistical authorities from European Member States, and other institutions that have been granted access through an application form. In order to work with the data, the following conditions must be met: a) The primary mission of the institution (or the relevant part thereof) is to conduct statistical or scientific research, b) results of the research will be published, and c) the institution has a good name and reputation.
Foreign processors	Foreign institutions can apply for access and should preferably have working relations with a Dutch authorised institution.
Data fees	The fees which apply to microdata research depend on the number of participating researchers, the number of dataset subjects and the duration of the project, among others. Services during the project start-up consist of a basis starting up cost of 1,800 EUR and an additional fee of 180 EUR per dataset topic. Importing one's own data will depend on the level of encryption, from simple (250 EUR) to complicated (1,300 EUR). Services during an ongoing research project are in part variable, depending on the data set topics (18 EUR support costs per topic) and output checking (220 EUR per output).
Pseudony-misation / anonymisation	Pseudonymised data is accessible in a secure remote environment with a personal token. The researcher can link CBS data with other datasets upon request. Only statistical output can be exported, and CBS checks whether results imply a risk of re-identification.

** Sources of information: cbs.nl, legal technical survey, knowledge of the authors*

Box 7.7	**BIGAN Health Research Infrastructure, Aragón, Spain**
Description	BIGAN integrates a technological infrastructure and a data lake gathering individual population and patient data from the regional health service and health related information systems from Aragón. Specifically, for research, BIGAN has put together healthcare data from 1.3 million lives – Aragón population, more than 800 million records in a data lake of pseudonymised patient data and renders it accessible to the scientific community as a one-stop shop service. The holistic approach gathering not only health data but also health related data (social, environmental, geographical) provides cross-fertilisation from various research areas which in turn might provide insight to future research policies.
Background	First mention of the ideas supporting the project BIGAN was introduced within the policy agenda through the Plan "Aragón Health-2030". This plan included a regional strategy for the common exploitation of all the health and health related information systems in Aragón with big data and AI tools; thus, harnessing the potential of the reuse of real-world (big) data (RWD) in Aragón for population health research.
Legislation	BIGAN was created as a new subsystem within the existing health information system in Aragón. Executive order (SAN/1355/2018) established the Aragón Regional Health Authority BIGAN platform. BIGAN platform is a data infrastructure implemented to reuse any kind of existing data for planning, quality management and health research. As an element of the health information system in Aragón, BIGAN platform is governed by the Health Law of Aragón (Law 6/2002), the Decree on social and healthcare information system (Decree 164/2000) and the Law on Research and Innovation in Aragón (Law 17/2018). Furthermore, BIGAN research complies with Law 41/2002 Governing Patient Autonomy and Law 14/2007, on biomedical research, and with national and European data protection legislation.
Tasks and activities	BIGAN overcomes research fragmentation and duplication by integrating health and health related data from the Aragón region into a single centrally managed

	infrastructure based on the modular design of the BIGAN platform that allows for increasing numbers of data sources to be integrated. BIGAN offers different portals according to its goals and required functionalities: Planning and Quality Management, Research, and Training. They are being deployed at different timespans. BIGAN Planning and Quality Management services started off in 2019, while BIGAN research and BIGAN training services are scheduled to be fully operational in 2021. From inception (2017) to full operation and evaluation (expected 2022), the deployment project has a forecasted duration of 5 years.
Governance	BIGAN is led by the Health Sciences Institute in Aragón (IACS). IACS was created by the Regional Health Law (6/2002), and is a public independent entity within the Health System in Aragón responsible for overseeing, promoting and managing biomedical research and innovation and producing evidence-based guidance on health technology, health policy assessment, and medical practice guidelines. BIGAN Oversight Committee controls and follows up BIGAN development according to its goals while IACS is in charge of the day-to-day operations. The Ethics Committee for Research in Aragón (CEICA) is responsible for ensuring the correct application of the methodological, ethical and legal principles in BIGAN activities including the assessment of the implications for individual and civil rights, distributive justice, health and safety and quality of life. In BIGAN, patients are able to view and change their data opt-out choice at any time (and without any justification needed).
Organisation and budget	BIGAN data controllers are the Aragón Regional Health Authority (Department of Health) and the Aragón Health Service (SALUD). Contracts between controllers and processors are in place, the last of them signed in February 2020. BIGAN infrastructure has an available budget of 1.06 million EUR for the period 2018-2020 divided in 3 categories (HHRR, IT and Subcontracting), HHRR being around 90% of the overall budget.
Staff and functions	The IACS Biocomputing unit (four members) is responsible for the design, operational management, development and maintenance of BIGAN infrastructure with the support of IACS staff on the IT, Legal, Ethical, and HHRR departments and with the assistance of researchers from the Health Services and Policy Research group.
Data sources and types of data	BIGAN research infrastructure data lake gathers individual level data from all the population registered as beneficiaries of the Aragón Health System (virtually 100% of the population) and the regional health service information systems, including primary care, specialised care, hospitalisations, ER episodes, drug prescription, drug reimbursement, image diagnosis, laboratory analytical determinations, diagnostics, vaccination, anamnesis and demographics. Data from these sources are updated according to their specific generation dynamics, in most cases daily.
Data users	According to the Protocol approved by the BIGAN Oversight Committee (December 2019), within the context of a research project, the pseudonymised data is accessible, directly to researchers within the "R&D Aragonese system" (as defined by regional law 17/2018); and indirectly accessible by other researchers (either public or private), when an agent of the R&D Aragonese system actively participates. Accessing BIGAN health research infrastructure includes a transparent approval process for health research projects which favours trust and accountability and fosters public-private partnerships and collaboration between public and private researchers, always under the assumption of the societal benefit of this collaboration.
Foreign data users	Favouring a seamless health data exchange in the European Research Area is an important objective of BIGAN research infrastructure and multi-country projects funded by national or European institutions are able to access to BIGAN research platform. Within the context of cross-border research projects, pseudonymised data is accessible by researchers (either public or private), when an agent of the R&D Aragonese system actively participates in the project. Non-R&D Aragonese

	agents can have granted direct access to the data although it requires a specific authorisation by the BIGAN Oversight Committee in the light of the criteria of relevance, security and social interest.
User fees	Basically the fees are composed of four categories, namely data extraction and data processing; computing; basic storage; advance storage, as follows: 1. Data extraction and data processing: 37.72 / 31.43* / 13.16** EUR/hour 2. Computing: 0.12 / 0.10* / 0.08** EUR/ hour /CPU 3. Basic storage: 0.93 EUR/year/GB 4. Advance storage: 2.67 EUR/year/GB * Reduced fee 1: applied to research projects managed by public research bodies or other public organisations. ** Reduced fee 2: applied to research projects managed by IACS, University of Zaragoza or the IIS Aragon Foundation Please notice that BIGAN research and training services are scheduled to be fully operational in 2021.
Pseudony-misation /anony-misation	The BIGAN data lake contains already externally pseudonymised data only. Re-identification of data at origin may take place only when, in the course of a research using pseudonymised data, it becomes apparent that there is a real and specific danger to the safety or health of a person or a specific group of people, or a serious threat to their rights, or that it is necessary to ensure proper health care.

** Sources of information: correspondence with relevant experts.*

Box 7.8	**Danish health data governance landscape**
Introduction	Denmark is a digitalised and data-intensive country and promotes actively data based research. As Denmark has a very rich and diverse health data governance landscape, this box outlines the main national infrastructural access points. In Denmark there is a difference between clinical access points and research access points. Sundhed.dk is the access point to EHRs for patients and also for health professionals for clinical purposes. A stakeholder needing data for research has several access points, and can go to the Danish Clinical Quality Program (RKKP) for quality databases, the Serum Institute for health data, and to Statistics Denmark for registry data combined across sectors.
Clinical care data	Primary care data must be accessed through the municipalities (for homecare and nursing homes) and DAK-E/KIAP from the Danish Quality Unit for General Practice for GP-data. Sundhed.dk is an independent agency governed by the Regions and the Government and contains the national EHR. At the sundhed.dk platform patients can access personal health information from EHR, laboratories, personal choices (e.g. organ donor), and the national patient registry. The patients can access their record, but they cannot report data or control the data. Health professionals also have access to the EHR.
Registry data	The two main national data governance bodies that host health data are: **Statistics Denmark**, storing data about the wider Danish population, and the **Danish Health Data Authority** (Sundhedsdatastyrelsen), hosting disease registers and data bases with health related information. Statistics Denmark is a public independent agency and holds copies of register data and can extract health data and combine it with social conditions when the researcher requests it. Researchers can apply for access to data locally with data custodians, or for the whole country through the Researcher Service (Forsker-service) at Serum Institute (when it is health data only) and through Statistics Denmark, if the researcher wants to combine health data with other data types. The Danish Health Data Authority holds all health registers, and provides research support service (Forskerservice) for researchers who wish to access health data. It is also responsible for national coordination of data exchange

	systems and infrastructures for the provision of healthcare. The Danish Clinical Quality Program (RKKP) is the cross-regional network organisation of the five Danish regions that constitutes the infrastructure of clinical quality registries and coordinates access to the data for researchers. The decision regarding access is made by the steering group of the individual data base. There is a fee for accessing data for research that must be paid to Statistics Denmark, the Serum Institute, or DAK-E but that only covers the hours spent on setting up the specific data set, and for DAK-E also the commercial vendor fee. It is not the cost of the infrastructure. Registry data are available for research with no informed consent ("solidarity by law").
Biobank data	The National Biobank, hosted by the Staten Serum Institute, and the Regional Biobank Program provide access to tissue samples. The National Genome Centre provides access to genomic data. The Health Act specifies that all genomic data from comprehensive genetic analyses is stored in a national genomic database and that patients have the right to opt-out of further use of the data.
Data exchange	All data is exchanged via the platform Sundheddatanettet. Data are not stored there but it is a secure space where you need authentication and approval to be linked up through VPN-access so that you can exchange data. MedCom is responsible for developing and setting standards for data exchange and testing supplier products before they are released to ensure data compatibility.
Data altruism	In Denmark Sundhed.dk mentions in their strategy for the coming two years that they wish to open up safe spaces for storage of citizen generated data, and potentially they can be marked as available for research too, but this is not operating yet.
Access by foreign researchers	Statistics Denmark has been involved in several working groups to facilitate data exchange between different countries. Data from Statistics Denmark is as a main rule only available for Danish researchers, but foreign researchers can get access to micro data through an affiliation to a Danish authorised environment. The Danish Health Data Authority applies the same rules.
User fees	There is a fee for accessing data for research that one has to pay to Statistics Denmark, the Danish Health Data Authority, the Serum Institute, or DAK-E (for GP data) but that only covers the hours spent on setting up the specific data set, and for DAK-E also the commercial vendor fee. It is not the cost of the infrastructure. While the exact situation is difficult to assess, a direct consultation with Statistics Denmark about calculation of prices does not suggest differentiated prices. However, public entities rarely pay for data access; they use the data they already have in-house, and do not order data sets through research service portals.
Pseudony-misation /anony-misation	All public agencies store data of citizens using the patient's ID number (PIN) and they can be linked at Statistics Denmark. They also link data from different sectors. Data held in the data access infrastructures are marked with a pseudonym of the patient's ID number (PIN).

** Sources of information: legal technical survey by national country correspondent, correspondence with relevant experts, van der Wel et al (2019), respective organisation websites.*

8. POTENTIAL ACTIONS AT EU LEVEL

8.1. Introduction

The findings of the surveys with country correspondents and stakeholders, as well as the workshops, as reported in the preceding chapters highlight a number of issues that impact the way in which health related data are collected and used. We have discussed the issues through the lens of three main functions for the use of health data: primary use for direct patient care, secondary use to support the safe and efficient functioning of healthcare systems, and secondary use to drive health research and innovation.

As well as collecting detailed information on the current legislation in place in the Member States, and how that legislation is perceived, the surveys and workshops also asked participants to explore possible action at EU level to overcome some of the hurdles in using data in the three function categories described.

In the following paragraphs we report on the discussions in the workshops and the survey findings on four interlinked potential areas of further EU level action:

- An EU level Code of Conduct;
- New health sector specific EU level legislation
- Non-legislative measures including guidelines and policy actions
- Practical measure to support a European Health Data Space.

It is important to note that the actions listed above are seen as being cumulative and/or complementary, and that ideally a mixture of all four would be developed to support the full range of data use models covered within the three broad functions of health data use. Furthermore, although the focus here is on EU level action, any such initiatives would have to be supported in some way at Member State level; whether through formal voting on a legislative proposal or Member State level support actions. This is of key importance not only to ensure uptake, but also to respect the balance of powers between the EU and Member States in accordance with the Treaty on the Functioning of the European Union.

In the sections below we first set out the four potential types of action, and then present the opinions of the country correspondents and stakeholders on their potential use as they emerged from the surveys and workshops.

8.1.1. An EU level Code of Conduct

Chapter 4 (section 5) of the GDPR provides for the potential development of various soft law tools that could support the application of data protection rules, these include Code of Conduct (Articles 40 and 41) as well as certification tools including data protection seals and marks. As noted in the European Commission's Communication on the Data Strategy (2020a), the EHDS could benefit from an EU wide Code of Conduct developed in accordance with Article 40 GDPR to provide clarity and guidance to the controllers and processors of personal data in the health sector on the application of EU wide data protection principles. Such Codes could be used to support legislative measures or as stand-alone measures to be applied where EU legislative action is less feasible.

A Code of Conduct is a voluntary accountability tool that helps to set out specific data protection rules for categories of controllers and processors, serving as a guidebook, providing operational meaning to the principles of data protection set out in the GDPR.

As such, a Code of Conduct can contribute to the proper application of the GDPR and support compliance with the GDPR (EDPB 2019b). Drafting a Code of Conduct in the

health sector is often seen as best achieved as a bottom-up process led by the primary stakeholders, researchers, privacy experts and patients. However, to be recognised as a Code of Conduct within Article 40, such a Code needs to be endorsed by the Data Protection Authority of the Member States in which it is to apply in accordance with procedure set out in Article 55. Where such a Code relates to processing activities in several Member States, the Code must be submitted by the competent Data Protection Authority to the European Data Protection Board, in accordance with procedure in Article 63, which shall then provide an Opinion (Article 40(7)). Where the European Data Protection Board confirms that the draft Code complies with the GDPR, the Board shall submit the Code to the Commission, who, by way of an implementing act may give general validity to the Code at EU level.

According to Litton (2017), a Code of Conduct can enhance transparency throughout research. A Code of Conduct should be written in simple language, given that legal texts can often be difficult to comprehend for non-lawyers. A Code of Conduct for the use and re-use of health data could give clarity and common rules about certain concepts included in the GDPR, such as anonymisation and pseudonymisation, which may benefit from further EU wide interpretation and clarification. It could also address issues such as the nature and format of consent in the context of observational research with personal data (as opposed to clinical trials), to provide better understanding of the interpretation of the consent to the use of data in scientific research as noted in recital 33 which, as the EDPB has noted, brings some flexibility to the degree of specification and granularity of consent in the context of scientific research, which may include processes to allow data subjects to consent for a research purpose in more general terms at the beginning and consent for subsequent steps in the project can be obtained before that next stage begins. A Code of Conduct would also be helpful to provide clarity and harmony in relation to the use of consent as a safeguard. Understanding in which circumstances it might apply and also the type of the consent that should be used in this context. It would be beneficial to provide clear delineations between consent within the meaning of the GDPR, informed consent standard at national level and informed consent as set out in the Clinical Trials Regulation and to set common rules around appropriate usage. A Code of Conduct could be key to setting out clear processes and standards for such a stepwise approach. A Code of Conduct could be instrumental in addressing the relationship between collaborative research, both within and between Member States, giving more clarity to the implementation of joint controllership as provided for in Article 26 GDPR. As noted in Article 40(3), such a Code of Conduct could also be used to govern collaboration between researchers in the EU and those in third countries. It should be noted however that a Code of Conduct has limitations and cannot change or replace existing legislation. With a Code of Conduct, researchers will still need to consult national law for the specific conditions under which patient data may be released for research in that Member State. Furthermore, unless constructed in close collaboration across all Member States, a risk exists that a European Code of Conduct could include elements that are at variance with national legislation adopted pursuant to GDPR. However, if such possible variances can be raised in the process of drafting a Code of Conduct, the resulting Code could be a very useful complement to both the GDPR and national legislation.

A Code of Conduct on the use of health-related data at EU level could therefore represent a strong tool to support trusted health data use and re-use and contribute to understanding and proper application of the GDPR in the health sector. However, it could have quite a long path from initial idea to final adoption through an EU level implementing act. And while it could be very useful, it would not solve all the issues that the surveys and workshops raised, as Dove (2018) observes: "Ultimately, even beyond the development of a Code of Conduct for Health Research, greater international

coordination is needed to seek legal interoperability across countries and regions, both within and outside Europe. The basis for that coordination, though, should be the GDPR rather than other data protection laws that provide weaker rights for citizens."

8.1.2. New sector specific EU level law

As noted above, a Code of Conduct could be given an EU level legal status through an implementing act, which is a legally binding act that enables the Commission to set conditions that ensure that EU laws are applied uniformly. However, other legal acts could also be envisaged at EU level to provide a harmonised approach to health data processing, addressing data governance principles, responsible use of health data and health data accessibility. The legislative measures could be complementary to the Code of Conduct.

Legislative measures could include EU level law based on article Art 114 TFEU on the functioning of the internal market, as well as legislative measures based on Art 168 TFEU on incentive measures to protect human health and in particular to combat the major cross-border health threats. The function of the eHealth Network established under Article 14 of the Directive on Cross-Border Care (2011/24/EC) could also be re-examined to establish if that group, or another EU level advisory group or groups, could play a role in supporting EU level action to promote better use and re-use of health data across the three functions explored in this report.

The experience of COVID-19 has shown an appetite for greater EU level collaboration to ensure that the EU is ready to respond to future pandemics. This change in perspective on the part of some EU stakeholders, as well as the engagement of the EDPB on issues such as contact tracing in COVID, could provide a useful impetus to explore the potential of these two legal bases to develop new EU level legislation that addresses the issues highlighted by the country correspondent and stakeholders in this study.

The European Strategy for Data, published in February 2020, foresees the creation of European Data Spaces and the legislative framework for their implementation. On 25 November 2020, the Commission adopted a Proposal for a Regulation on European Data Governance (also known as the Data Governance Act), which will be negotiated by the co-legislators before formal adoption as an EU Regulation (COM, 2020b). The Data Governance Act has four key functions including allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR), and allowing data use on altruistic grounds.

The proposal for a Data Governance Act foresees that it may be complemented by sectoral legislation to address the specific needs of sectors, such as for re-use of health data. As such it provides an ideal opportunity to address some of the challenges for secondary use of data in functions 2 and 3 as described in this report. The proposed Act also foresees the creation of single information points for all the sectors (including the health sector), whose function it will be to redirect the requests for access to data to public sector bodies or other competent bodies that could support access to health data. It sets out a notification scheme for providers of data sharing services, with competent authorities which should cooperate with relevant sectoral authorities, as well as a registration scheme for data altruism organisations, whereby competent authorities cooperate with relevant sectoral bodies. Here again it will offer an opportunity to address some of the challenges explored in chapter 7 of this report.

The proposal for a Data Governance Act also sets out a European Data Innovation Board, which would comprise representatives of EDPB, the Commission, relevant data spaces

and other representatives of competent authorities in specific sectors. Among the activities of the Board, one can include activities aimed at supporting cross-sector data sharing, including interoperability of data and data sharing services between different sectors and domains, building on existing European, international or national standards.

The proposed Data Governance Act therefore creates an opportunity to develop sectoral EU level legislation for the European Health Data Space (EHDS), which could address not only the governance and infrastructure to allow for the primary use of health data for healthcare, as well as the secondary use of health data for research and policy making, but also facilitate data sharing within the EHDS in accordance with the GDPR. Such legislation should complement and build upon the Data Governance Act.

Learning from current developments at national level, this legislation could support single point of contact systems, similar to those explored in chapter 7, allowing for secondary use of health data at national level, whose cooperation would be supported at EU level in order to facilitate access to health data for cross-border research as well as for national and regional level research. At EU level, one could envisage a data permit authority or a similar controlled single-entry point to build a trusted environment for shared data access for certain pan-European types of data. These single points of contact could also be the sectoral contacts for single information points. A digital health infrastructure on secondary use of health data, linking data permit authorities, other bodies dealing with secondary use of health data, as well as public bodies such as EMA and ECDC should be set up. The details of such infrastructure could be set up in tertiary legislation. European level legislation would have the distinct advantage of building a robust and transparent governance structure, which could be supported at EU level to ensure strengthened cooperation between Member States (network, committee etc.) or by an EU-level body or agency created specifically for this purpose.

Noting again the need for EU data solidarity demonstrated by collaborative response to the COVID-19 pandemic, the Data Governance Act paves the way for the adoption of new EU level legislation to facilitate the means for individuals to make health data concerning themselves available to trusted researchers and setting up the right governance structures to manage such data. This legislation could also support easier access to health data for public authorities (medicine agencies, epidemiological institutions, public health institutions etc), based on article 9(2)(i) of the GDPR, supported by a strong governance at national and EU level. If appropriate, this could also include a simplified EU level process to allow use of pseudonymised health data, based on article 9(2)(j) GDPR and supported by a strong governance at national and EU level for the data management. In this context, the single points of contact could also be the contact points for bodies dealing with registration of data altruism organisations under the Data Governance Act.

In the context of data processing for patient care (as opposed to research) new EU level actions could be envisaged building on the Cross-Border Healthcare Directive (2011/24/EU). This could include revisiting the role of the eHealth Network, the advisory body created under Article 14 of the Directive. In the context of cross-border care this could be used as a mechanism for supporting data sharing across the EU, both for direct sharing between healthcare professionals and also to support patient in exercising the portability of their health data when they seek care in another EU Member State based on rights on the Directive 2011/24/EU.

Consideration could also be given to the technical interoperability issues inherent in sharing health data. While the European Commission has issued the Recommendation on a European Electronic Health Record Exchange Format (COM, 2019b), the interoperability of EHRs and other health data remains low in Europe, including with m-health/tele-health, both within and between Member States. New legislative measures could

therefore be considered, either through providing a concrete legislative follow up (implementing/delegated acts) to the guidance provided by bodies such as the eHealth Network, or possibly through other implementation measures in the Cross-Border Care Directive, to ensure that the promise of cross-border care can be underpinned by more easily shareable health information. This could include further development of EU level minimum datasets such as the Patient Summary, e-Prescriptions, with new elements such as images and image reports, laboratory results and discharge letters to be added later on, as well as measures to support the uptake of standards and specifications that should be respected when data moves cross-borders. To ensure interoperability intra-borders, the options can vary between labelling/notification/certification/authorisation schemes. Work is already underway in the context of the eHDSI / MyHealth@EU, which could be supported to further strengthen the mobility of data, including elevating the role of the National Contact Points for eHealth from voluntary to mandatory and increasing the scope of their role.

Taking into account the overall context of the data governance, in the health sector it seems necessary to set up sectoral bodies dealing with digital health, with tasks related to interoperability and its use for healthcare, but also tele-health, m-health and other tasks such as criteria for security of digital health infrastructures etc. Such sectoral health interoperability bodies could be the contact points for bodies dealing with notification of data sharing providers, but could also support at national level the interoperability between electronic health records, of EHRs with medical devices and m-health applications. Such support would also facilitate the decisions of the health authorities to prescribe and reimburse different m-health and tele-health solutions. These national bodies could also contribute at EU level to the decisions on standards and interoperability, security of data etc. They could be brought at EU level in a renewed type of legal body, that could select the standards, quality criteria etc., implementing at national level through labelling/notification/certification/ authorisation schemes. Such a body could also cooperate with a body dealing with secondary use of health data.

8.1.3. Non-legislative measures including guidance and policy actions

To complement the legislative measures and to support the development of the Code of Conduct, other non-legislative measures could be considered at EU level to further support the cooperation across the national borders.

Working within the framework of the GDPR, more guidance could be provided by the European Data Protection Board, in its capacity under Article 70, to ensure consistent application of GDPR. In this context the opinions of bodies such as the European Group on Ethics and the European Parliament's Panel for the Future of Science and Technology (STOA) could be also taken into account as well as interaction with researchers and patient organisations. A broad variety of stakeholder groups could be involved in the present debate on the EHDS, whether on the national or on the EU level, and appropriate platforms should be used or set up for that purpose.

Besides additional guidance on the legal requirements, significant collaboration is needed also on technical issues such as infrastructure, technical interoperability and also data quality and semantic interoperability. While most Member States have endorsed the concept of FAIR data (findable, accessible, interoperable and reusable), more efforts are needed at EU level to advance the objectives set out by the EC Expert Group on FAIR data (2018).

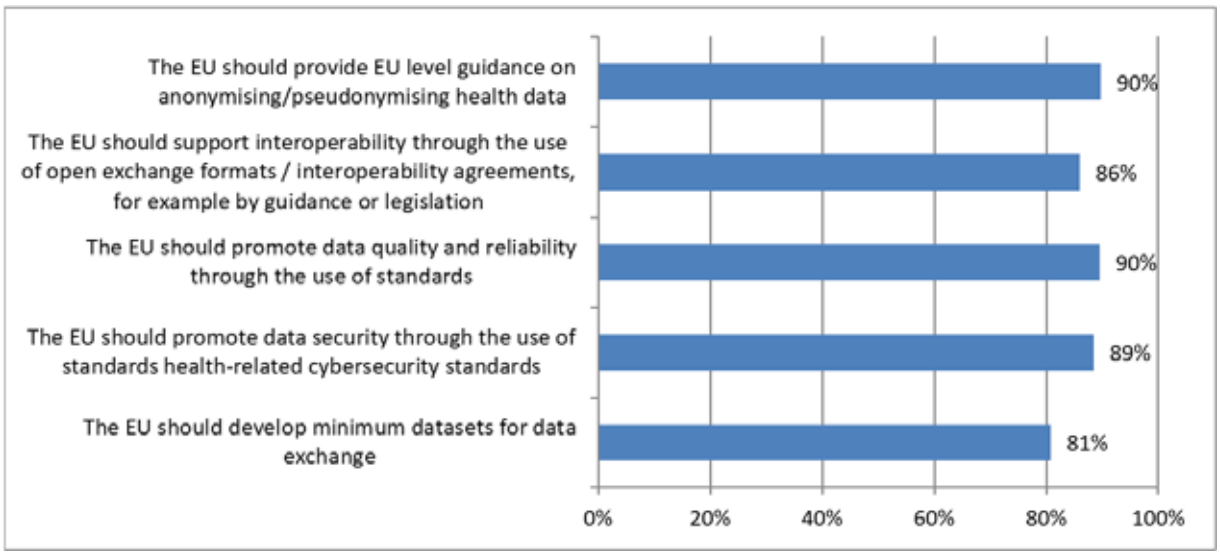
This could include, *inter alia*, more guidance on the inclusion of technical standards in public procurement tenders, where applicable. The recent Communication of the European Commission 'Guidance from the European Commission on using the public procurement framework in the emergency situation related to the COVID-19 crisis' (COM, 2020c) is a good example in this context. However, there can be a tension between FAIR and data protection, especially when the data processing is based on consent (Boeckhout 2020). Finally, by using the support from the appropriate financial tools such as the Connecting Europe Facility, Digital Europe Programme or the future EU4Health Programme, the EU could support more effective collaboration on building appropriate infrastructures, improving quality of health data and capacity building in the Member States that would further improve digitalisation and sharing of the data for research and health policy-making across borders.

8.2. Exploring Support for Action at EU Level

The results of the surveys as set out in the preceding chapters show that users of health data report problems arising from poor understanding of the exact meaning of the GDPR for their work. This is to some extent due to the fact that the GDPR is a horizontal legislation and as such does not address all the specificities of using health data for a range of legitimate purposes. Furthermore, the key articles of the GDPR that foresee the use of health data for health care provision, public health and research depend on national (or EU) level legislation. This in turn creates problems for cross-border use of data where different legal bases may be used and different requirements may be set in the national level legislation. The surveys showed that these issues create many problems and that there is broad support among stakeholders for EU level action to facilitate the understanding of the GDPR, to address the variations between Member State legislation and to address the need for more technical and sematic interoperability for data sharing.

Figure 8.1 below shows the results of a series of questions that were asked in the stakeholder survey with respect to a range of issues in which future EU level action might be considered. Below we explore the implications of some of those findings in several sections.

Figure 8.1 Share of stakeholders agreeing with the following statements, all related to potential actions that may be taken by the EU for the use of health data for healthcare, policy making and research



8.2.1. Anonymisation and pseudonymisation

The survey among stakeholders clearly shows that EU level guidance on data anonymisation and pseudonymisation is seen as needed, with 90% agreeing that EU level guidance should be provided. This sentiment was also echoed among workshop audiences, who called for greater coherence on the definitions of these terms and the tools used to achieve them across the EU.

It is important here to note that anonymisation is considered a useful tool for risk containment. Yet, anonymisation as such is still an act of data processing and must be legitimated under the GDPR. Therefore the collection of data must be legitimate under Article 6(1), and 9(2) GDPR and the processing to render the data anonymous must be justifiable, compatible with the purpose of which data was originally collected. Article 5(1) GDPR provides that where the further processing is, inter alia, scientific research such further processing shall not be considered incompatible if the further processing is conducted in accordance with Article 89(1) which requires that suitable safeguards are met. Clarifications are however needed under which conditions the further processing of data in order to render them anonymous for purpose of scientific research would be legitimate.

Furthermore, more clarification is needed on when data can really be considered anonymous. Recital 26 states that all reasonable means that may be used to identify a natural person from data must be considered. If the use of such reasonable means could identify an individual, then the data are not anonymous. Many authors have commented on the differences between the conditions according to which data may be considered anonymous as stated by the Article 29 Working Party in 2014 and the decision of the Court of Justice in Breyer in 2018 (Mourby, 2018, European Parliamentary Research Service - Scientific Foresight Unit, 2019; Groos and van Veen, 2020). A key challenge here will be the need for common understanding of anonymity to keep pace with scientific advance, the concept of 'reasonable means' as well the 'objective factors such as the costs of the amount of time required for identification' noted in recital 26 are heavily dependent on the state of the art of technology. The drafters of the GDPR were of course aware of this issue and hence noted the importance of recognising the development of technology that could impact on the capacity to identify an individual from data that may appear to be anonymous.

Notwithstanding the interests of some researchers in gaining more clarity on anonymisation, it will not provide an adequate data protection safeguard for all types of scientific research relating to health. In a situation where data are used for the primary function of providing care, anonymisation will be of very limited use, since the patient must be identified. However, it also poses problems in certain types of research where the ethical requirements of Research Ethics Committees often demand that a research participant can be notified if during the course of a trial or other research activity a finding is made that would have a material health impact for the research participant (this is referred to as an incidental finding). Pseudonymised data is therefore more commonly used in the healthcare setting because it can safeguard data while still allowing for identification if this is necessary. Since pseudonymised data falls within the remit of GDPR its definition and the tools used to render data pseudonymised should have a common interpretation across the EU if possible. Some countries set up groups of experts in pseudonymisation and this could also be useful at EU level, since a common understanding and approach is currently lacking in national and EU legislation.

In conducting risk assessment on the use of data by industry, pseudonymisation is a core element of this risk-based approach and risk balancing is key. The need for a common European understanding of the terms anonymisation and pseudonymisation and the current lack of certainty surrounding these terms make them ideal terms to be further defined in sector specific legislation and supported by non-legislative tools such as guidelines.

8.2.2. Security

Closely related to safeguarding tools like anonymisation and pseudonymisation is the need to common approaches to security, including cyber security, to ensure that when data are shared (both in a nominative and pseudonymised format) the safety of such sharing can be assured. Here the call for EU level action among stakeholders was at 89%, thus at almost the same level as the call for common action on anonymisation and pseudonymisation. This demands not only a common legal understanding of how terms such as 'security by design' should be understood, but also closer collaboration between Member States on technical aspects of security. The European Union Agency for Cybersecurity (ENISA) could play a role here and might not be sufficiently known to the stakeholders. EU level guidance on security is a good example of the need for close interplay between hard law and legal guidance documents. A legislative act, such as legislation on the operation of the EHDS, could call for compliance with security standards and for such standards to be mandated in any public procurement related to the operation of the EHDS. However, as data science is very fast moving, guidance documents of bodies such as ENISA, supported by national level implementation through national eHealth contact points, could ensure that the businesses bringing health data security solutions to market could more easily demonstrate compliance with EU law. It is often reported by data controllers that they struggle to satisfy themselves that the mechanisms of data security products fully satisfy the requirements of GDPR and related legislation such as the NIS Directive (2016/1148/EU).

8.2.3. Data quality and minimal data sets

Support for a minimum dataset to facilitate health data exchange was also expressed in the workshops. It was noted that within Member States, data are collected in different ways, so it is hard or even impossible to combine them in a useable way, therefore, initiatives to come to a common understanding on what data should be collected would be a significant advantage. Such initiatives should be pursued at Member State and EU level to find agreement on core elements of data sets in order to facilitate better co-operative use of such data sets for research and health system administration. Europe has already made significant advances in this domain with the adoption of the Patient Summary and e-Prescriptions that are supported within the eHDSI, as well as in the current initiatives to adopt common formats for disease registries for rare diseases in the context of the European Reference Networks on rare diseases. More initiatives could be envisaged leveraging the work commenced in the rare disease domain, here again a revised role of the eHealth Network could be considered.

8.2.4. Interoperability

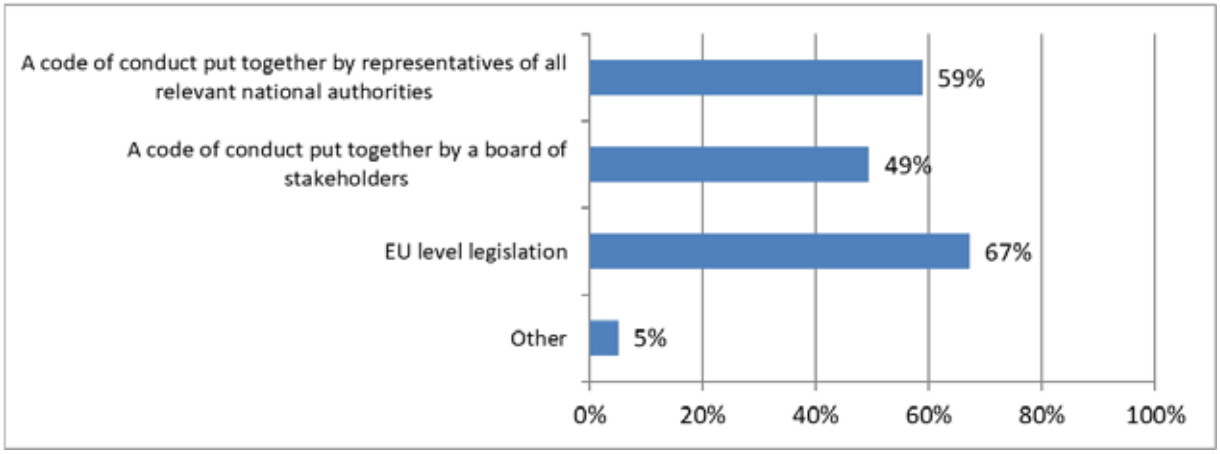
The issues described above all demand renewed action on semantic and technical interoperability. In order for data to be shared, whether for patient care or for research, the data must be shareable in a way that ensures their confidentiality, integrity and availability.

This demands that more effort is needed at both national and EU level to promote standards that ensure that data are collected in a way that allows them to be used across systems without compromising their integrity and ensuring their availability where needed. The Commission has put forward the Recommendation on European Electronic Health Record Exchange Format (COM, 2019b), but its implementation remains limited and further efforts are needed to strengthen interoperability, at national and EU level. While the GDPR itself does not address interoperability of data, certain provisions within in could be used to support better and wider use of technical standards in health data exchanges. Article 9(2)(i) for examples provides that Union of Member State law may be introduced to ensure suitable safeguards when data are processed in the interests of public interest in public health, noting that this may arise in protecting against serious cross-border health threats. The initiative on the European Health Data Space could foster the compliance with specific technical standards to ensure that such data can be shared across borders in an interoperable manner.

8.3. Views on a Code of Conduct

Based on the results of the stakeholder survey, a little over half of the stakeholders believe that the EU should intervene to help orchestrate health data sharing for secondary purposes at EU level through the means of a set of common rules, put together in a Code of Conduct (soft law) (see Figure 8.2). A clear Code of Conduct may reduce unnecessary fear about compliance and enhance data sharing for the sake of progress in research. It is important to note however that there was also a higher level of support among stakeholders for EU level legislation on health data sharing for secondary purposes (see Figure 8.2).

Figure 8.2 Share of stakeholder agreeing with the following statements, all related to how the governance of an EU level data sharing infrastructure should be assured if it was set up as



The potential for a Code of Conduct was addressed in the surveys and also addressed extensively in the workshops. It was seen, among other potential tools, as a means to help stakeholders in Member States understand the GDPR and its application in specific health related settings. A Code of Conduct at EU level could be particularly helpful in creating common rules in situation of data sharing between Member States, noting that differences necessarily arise because the GDPR allows for divergences in the way Member States implement it in the healthcare sector.

The workshops generally concluded that there is a need for a Code of Conduct, based on articles 40-41 of GDPR, in order to add legal clarity and give guidance to controllers, especially for secondary use of health data for scientific research purposes. However, a Code of Conduct should not exclude further EU measures to facilitate health data use in the public interest in the field of public health or for scientific research purposes. Stakeholders represented in the second workshop argued that those who use data should be actively engaged with the development of a Code of Conduct, noting that a balance is needed between those using data for the public interest and the interest of the patient. Patient representatives called for special attention to be given to the inclusion of patients and patients' representatives in the development of a Code of Conduct.

Workshop participants noted also that a clear EU level legal framework will be important for the secondary use of data, and in particular for the development and functioning of the European Health Data Space. Such a framework should provide clarification of the relevant requirements under GDPR, as well as on the Guidelines and case law around that GDPR that are beginning to emerge. With reference to using a Code of Conduct as part of this legal framework, it was noted that there are several organisations and projects (WHO, EMBL, BBMRI, 1MGP) and national initiatives that could be a starting point, and that a new EU level initiative should not start from scratch.

Questions concerning the potential for a Code of Conduct were also asked in the legal surveys. Here the country correspondents stressed the need to develop a unified understanding of key concepts in the GDPR, such as legal basis, controllership, definition of personal data, pseudonymisation versus anonymisation, as a first step, and then build on that understanding with further specific legal guidance. Country correspondents also pointed to the fact that while there are limitations to a Code of Conduct, it could give a shared interpretation of provisions in the GDPR which are valid without national implementation such as 5.1b or 17.3d GDPR. It was noted that this could be developed as a single Code of Conduct with applicability across the EU (if so endorsed by an implementation act), or as baseline Code of Conduct with national appendices for each MS, which would then have to be approved by the DPA in each MS.

It was noted that some steps towards clarification of terms had been taken, notably in the questions and answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation published by the European Commission in May 2019 (COM, 2019a). While this provides some useful starting elements, many terms still demand clearer guidance. A Code of Conduct could play a role in offering such clarification, but ideally such clarification would come from the EDPB, based on which a Code of Conduct could be developed to address some of the specific procedural issues in the use health data for purposes such as further research.

8.4. Views on future legislation

Throughout the three workshops, participants stated that both hard and soft laws will be needed at the EU level, as not all current issues can be solved by soft law. This conclusion is in line with the results of the stakeholder consultation, which also favoured a mix of legislative approaches.

As noted in the introduced, EU level legislation could be created based on the provisions for legislation in support of the functioning of the internal market (Article 114 TFEU) or in support of public health (Article 168 TFEU). However, the GDPR itself foresees the potential EU level legislation in the context of the legitimation of processing of health data in certain circumstances, notably for processing data in the public interest (Art

9(2)(i) GDPR) and processing for scientific research purposes (Art 9(2)(j) GDPR). Participants in the workshops observed that the adoption of such legislation could be very useful in fostering common approaches by Member States in their implementation of both sub-articles. However, such legislation would need to take heed of the Treaty provisions in Article 168(7) that Union action shall respect the responsibilities of the Member States for the definition of their health policy and for the organisation and delivery of health services and medical care. Furthermore such legislation would also have to be compatible with national level sectoral law on the organisation of health systems, including the capacity to address both public and private entities conducting research. Mindful of the rules of subsidiarity one of the country correspondents argued that EU legislation under Art. 9(2)(i) or (j) GDPR could be developed to guide the setting up of the (preferably) federated infrastructure for EU level data sharing, defining the governance of such an infrastructure including the roles of EU and Member State bodies. This could be drafted to deal with access rights and management and tackle exercise and enforcement of data subject rights. The proposal for a Data Governance Act, adopted based on article 114 TFEU, sets out a minimum common denominator that may be further enriched with sectoral legislation, for instance in the area of health to reply to the needs of the EU healthcare systems.

The discussion in the workshops also considered if action could be taken at EU level, in particular with respect to the right of data access and portability. The Regulation on the coordination of social security systems (883/2004) as well as the Directive on Cross-Border Care (2011/24/EC) create the right for patients to receive care in another Member States in certain circumstances, with the Regulation being focused on planned care provided by a public health care provider with the financial aspects handled between the relevant Member State authorities, and the Directive addressing both planned and unplanned care provided by all types of healthcare providers, based on a system of patient reimbursement of costs up to the level that would have been reimbursed in their home system. The Directive foresees care being provided in person or remotely and creates also the European Reference Networks for Rare Diseases to allow knowledge on rare diseases to be shared across the EU for the benefit of patients. Whether a patient travels expressly to receive care, is treated remotely or falls sick unexpectedly and needs to receive care while travelling, in all cases the care will be better if it can be supported by easy access to the patient's medical files. This demands that a patient can access and share their EHRs and other files and in some cases also requires data to be portable so that it can be transferred directly to a care provider in another Member State. The eHealth Network and the eHealth Digital Services Infrastructure are developing important tools to help make data access and portability easier, including through the Commission's European Commission Recommendation on the European Electronic Health Record exchange format (COM, 2019b) which seeks to facilitate the cross-border interoperability of electronic health records (EHRs) in the EU by supporting Members States in their efforts to ensure that citizens can securely access and exchange their health data wherever they are in the EU. The Recommendation supports the digital transformation of health and care in the EU by seeking to unlock the flow of health data across borders.

The Recommendation is an important practical tool, but it lacks the strength of EU level legislation that expressly addressed the right of patients to share their health records with healthcare providers in other EU Member States. Given that the Regulation on social security and the Directive on Cross Border Care both implicitly recognise the need for patients to be able to share records, it was noted that it may be worth considering if it offers an avenue for a legislation to address cross border health records access and portability. Alternatively, one could look at the matter from an internal market perspective, arguing that without safe and reliable means to ensure that health records

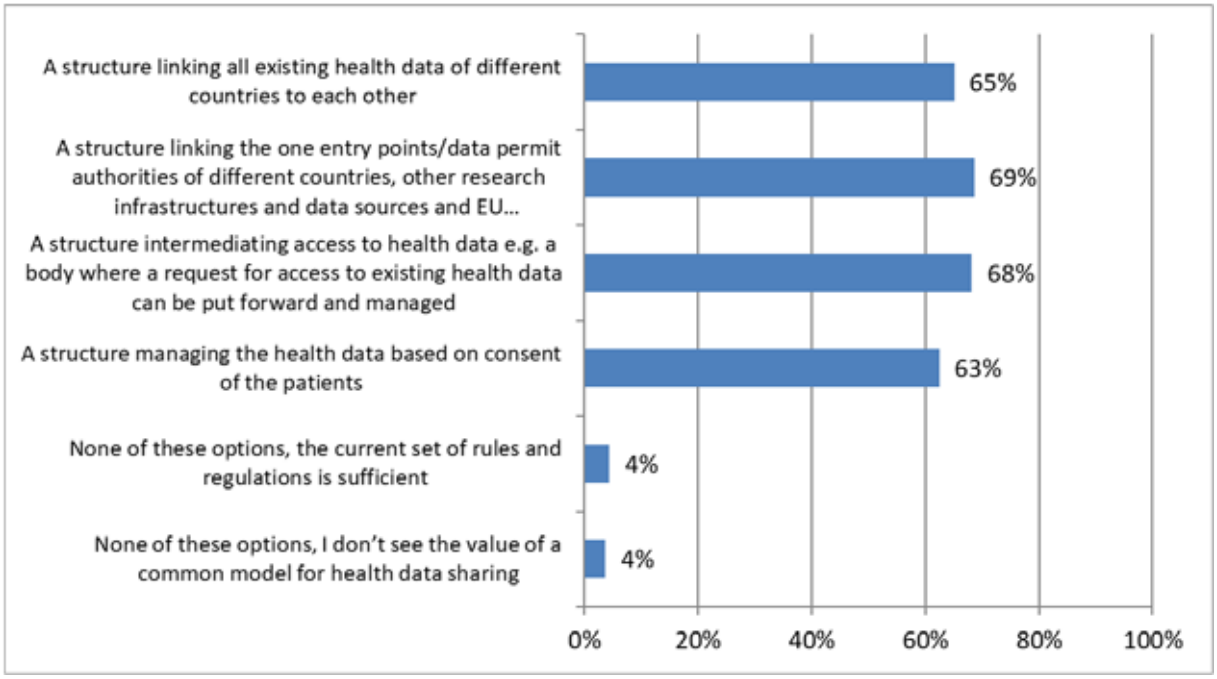
are shareable by patients with healthcare providers of their choice, the right to freedom of movement enshrined in the Treaty on the Functioning of the European Union are hampered and that legislation should be adopted under Article 114 of the which addresses the functioning of the internal market.

The wealth of discussion on the use of a range of legal basis to adopt EU level legislation demonstrates a significant level of support amongst Member State level experts and a range of EU level stakeholders for both Codes of Conducts and legislative action at EU level, with both being seen as core tools for overcoming differences in interpretation of the GDPR and supporting the use of data for both patient care and all types of research.

8.5. Addressing the practical needs of a European Health Data Space

As well as legislative measure, the workshops and surveys explored options for practical tools to support the use of health data across the three functions as defined within the study. This included the polling of opinions by stakeholders for different issues to be addressed by an EU level structure (Figure 8.3 below), showing broad support for all variations in approach, with a slight preference for an infrastructure to create a single entry point to give researchers a facility for gaining trusted access to the data sets held in other EU countries.

Figure 8.3 Share of stakeholders agreeing with the following statements, all related to the types of functions an EU level data sharing infrastructure for secondary purposes should have, if it was set up



The options suggested in the poll are all elements which could be addressed in the context of the creation of the EHDS, to foster access to different kinds of health data (electronic health records, genomics, registries, etc.) in Europe with full respect to the GDPR. In the workshop, there was consensus concerning the need to develop new tools to support the cross-border delivery of healthcare, as well as the use of health data for the development of new treatments, medicines, medical devices and services. It was noted that this was needed to meet the needs of different users and actors in the system (healthcare providers, researchers, industry, policy makers), whilst simultaneously protecting citizens' data. In another workshop that brought together European level

stakeholder bodies, the need for such infrastructure to ensure compliance with the FAIR data principles was brought to the front.

Noting the interest in the development of an EU level infrastructure to support access to data for secondary data use purposes in the workshops, some of the issues raised in those discussions were developed further in the surveys. We looked in particular at the type of structure that stakeholders would favour and the partners who should be included in its development.

Figure 8.4 below shows that an EU Agency is seen as the preferred model which could be supported by an EU level committee or other body which ensures close interaction between the relevant Member State bodies. Figure 8.5 demonstrates clearly that stakeholders call for representatives for all sectors involved in health care consumption, delivery and regulation to work in close co-operation in the design of an EU level legislative tool or infrastructure designed to support the secondary use of health data across the European Union.

Figure 8.4 Share of stakeholders agreeing with the following statements, all related to how EU level data sharing infrastructure for secondary purposes should be organised, if it was set up

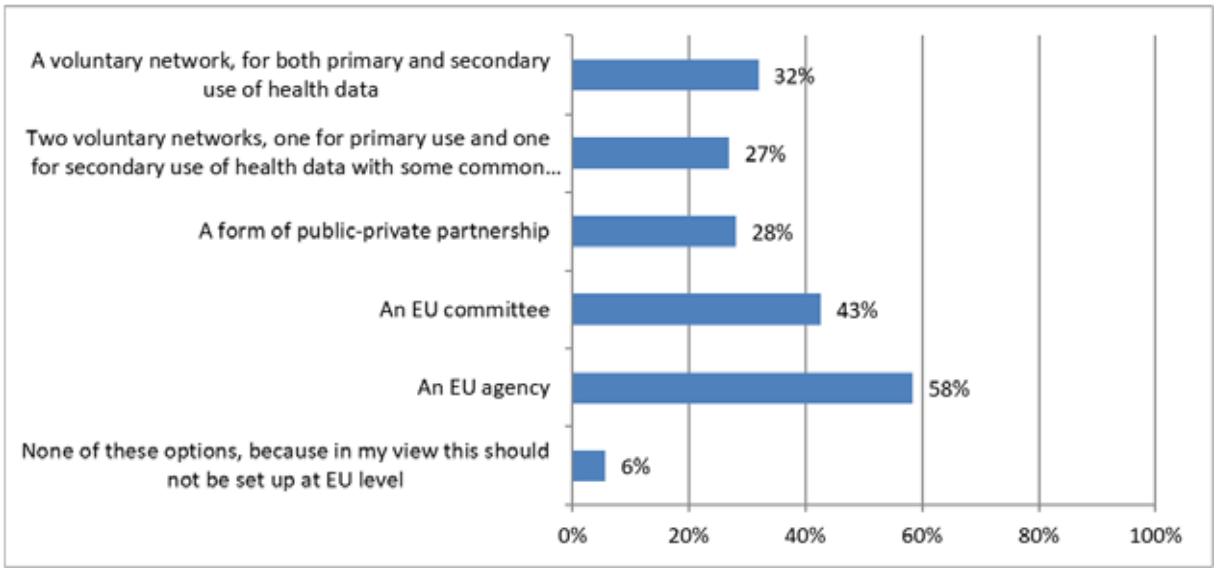
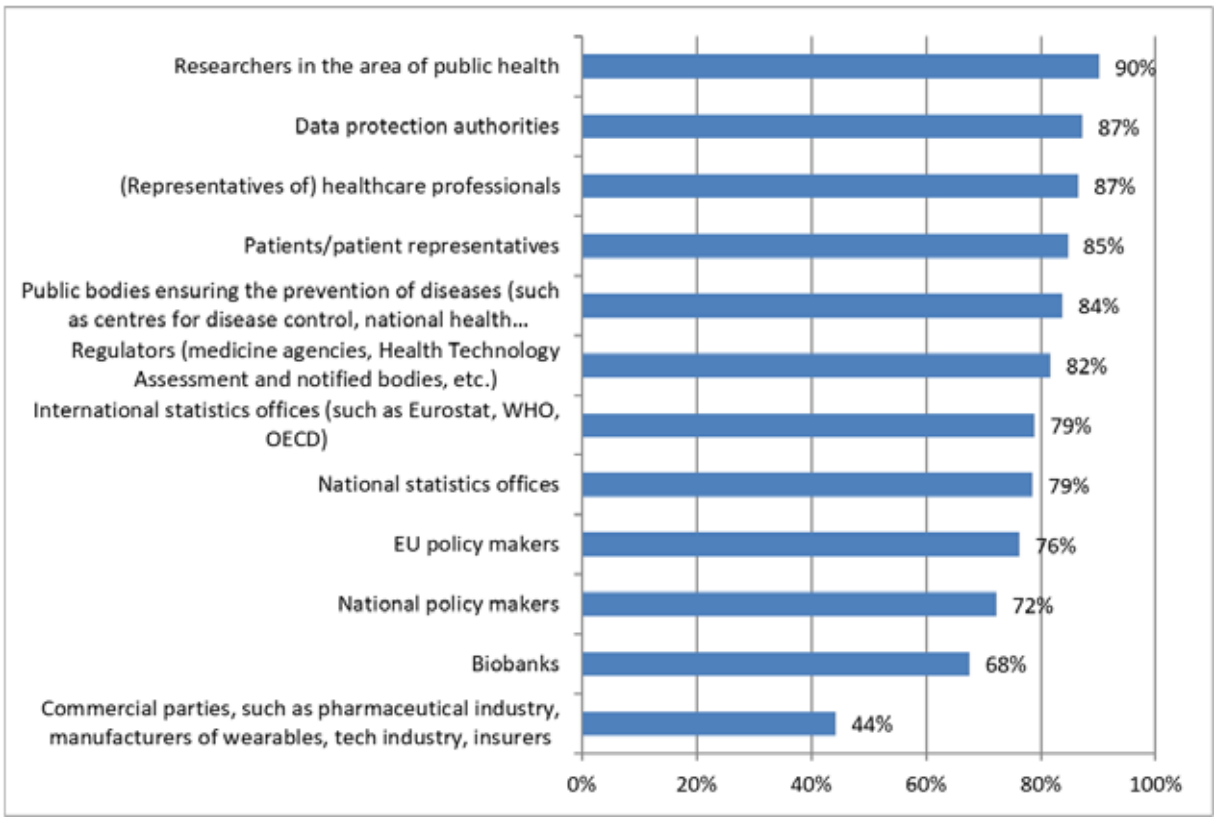


Figure 8.5 Share of stakeholders agreeing with the following statements, all related to who should be involved in setting up regulations for the secondary use of data at European level



8.6. Conclusions and next steps

The work conducted in the context of the study makes clear that a number of legal and operational issues need to be addressed to ensure that European healthcare systems can make best possible use of data for the three interlinked purposes of primary use for direct patient care, secondary use to support the safe and efficient functioning of healthcare systems, and secondary use to drive health research and innovation. It is clear from the evidence of workshop participants, country correspondents and stakeholder consultation that while the GDPR is a much appreciated piece of legislation, variation in application of the law and national level legislation linked to its implementation have led to a fragmentation of the law which makes cross-border cooperation for care provision, healthcare system administration or research difficult. Furthermore, the interpretation of the law is complex for researchers at national level and patients do not always find it easy to exercise the rights granted by the GDPR.

Findings from the study also show a strong support for the work on the EHDS, but highlight that such a system would require a sound level of legal and operational governance and a clear common understanding of the concepts of the GDPR.

It is clear that addressing these challenges requires a multifaceted approach. The identified future EU level actions to address these challenges, that should be complementary and cumulative, include stakeholders driven codes of conduct, new targeted and sector specific EU level legislation, guidance and support to the cooperation among Member States and relevant stakeholders, but also support for digitalisation, interoperability and digital infrastructures, allowing for the use of data for healthcare,

policy making and research and innovation. It is important that these future actions are developed in full respect of principles of proportionality and subsidiarity.

Whatever next steps are chosen by EU policy makers, it is clear that co-operation between Member States is crucial. Such co-operation should also fully take into account the interests of the key stakeholders, in particular patients, healthcare professionals, healthcare providers, researchers, industry and also health and data protection authorities. The COVID-19 pandemic has clearly demonstrated the need for such co-operation and provided many examples and new models that can bring rapid, responsive and impactful action that should be further developed in the future.

As a final word, it is important to note that sound health data governance will be one of the pillars of trust that support the European Health Data Space, but it can only be successful if it is truly supportive of the other pillars of trust which demand assurance of data quality, transparency, and the full support to patients to act as active agents in their own health and care, with full capacity to exercise their health data related rights.

REFERENCES

Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymisation Techniques. 0829/14/EN. WP216

Ballantyne, A. (2020) How should we think about clinical data ownership? J Med Ethics;46:289–294

Bensemmane, S. and Baeten, R. (2019), Cross-border telemedicine: practices and challenges. OSE Working Paper Series, Research Paper No.44 Brussels: European Social Observatory, October, 63p.

Blumenthal S. The Use of Clinical Registries in the United States: A Landscape Survey. EGEMS (Wash DC). 2017;5(1):26. Published 2017 Dec 7. doi:10.5334/egems.248

Boeckhout M., Zielhuis G.A., Breedenoord A.L., The FAIR guiding principles of data stewardship : fair enough ? European Journal of Human Genetics, vol. 26, iss. 7, (2018), pp. 931-936, https://doi.org/10.1038/s41431-018-0160-0

Boeckhout M., Beusing M., Bouter L., et al. (2020). Niet-WMO-plichtig onderzoek en ethische toetsing. Antoni van Leeuwenhoek & MLC foundation.

Castell, S., Evans, H. (2016). The one-way mirror: public attitudes to commercial access to health data. Ipsos Mori, Wellcome Trust.

Chassang G., Southerington T., Tzortzatou O., Boeckhout M., & Slokenberga, S. (2018). Data portability in health research and biobanking: legal benchmarks for appropriate implementation. Eur. Data Prot. L. Rev., 4, 296.

Chico, V. (2018) The impact of the General Data Protection Regulation on health research, British Medical Bulletin, Volume 128, Issue 1, December 2018, Pages 109–118, https://doi.org/10.1093/bmb/ldy038

Clarke, N., Vale, G., Reeves, E. P., Kirwan, M., Smith, D., Farrell, M. & McElvaney, N. G. (2019). GDPR: an impediment to research?. Irish Journal of Medical Science 188(4), 1129-1135.

Coebergh J-W, C van den Hurk, M Louwman, H Comber, S Rosso, R Zanetti, L Sacchetto, H Storm, E-B van Veen, S Siesling, J van den Eijnden-van Raaij (2015) EUROCOURSE recipe for cancer surveillance by visible population-based cancer RegisTrees® in Europe: From roots to fruits. European Journal of Cancer, 51-9: 1050-1063.

Cole, A. and Towse, A. (2018) Legal barriers to the better use of health data to deliver pharmaceutical innovation. OHE Consulting Report, London: Office of Health Economics. https://www.ohe.org/publications/legal-barriers-better-use-health-data-deliver-pharmaceutical-innovation

Cool A. (2019) Impossible, unknowable, accountable: Dramas and dilemmas of data law. Soc Stud Sci. 2019;49(4):503-530. doi:10.1177/0306312719846557

Courbier S., Dimond R., Bros-Facer V. (2019). Share and protect our health data: an evidence based approach to rare disease patients' perspectives on data sharing and data protection - quantitative survey and recommendations, Orphanet Journal of Rare Diseases (2019) 14:175.

Crico, C., Renzi, C., Graf, N., Buyx, A., Kondylakis, H., Koumakis, L., & Pravettoni, G. (2018). mHealth and telemedicine apps: in search of a common regulation. ecancermedicalscience, 12.

Cruz-Correia, R., Boldt, I., Lapão, L., Santos-Pereira, C., Rodrigues, P.P., Ferreira, A.M., & Freitas, A. (2013). Analysis of the quality of hospital information systems audit trails. BMC medical informatics and decision making, 13(1), 84.

Deliversky, Jordan, and Mariela Deliverska. "Ethical and Legal Considerations in Biometric Data Usage-Bulgarian Perspective." Frontiers in public health vol. 6 25. 12 Feb. 2018, doi:10.3389/fpubh.2018.00025

Delvaux, N., Aertgeerts, B., van Bussel, J.C.H. Goderis, G., Vaes. B, Vermandere, M. (2018) Health Data for Research Through a Nationwide Privacy-Proof System in Belgium: Design and Implementation. JMIR Med Inform 2018;6(4):e11428) doi: 10.2196/11428

Dove, ES 2018, 'The EU General Data Protection Regulation: Implications for international scientific research in the digital era', Journal of Law, Medicine and Ethics, vol. 46, no. 4, pp. 1013-1030. https://doi.org/10.1177/1073110518822003

Dickenson, D. (2013) Me Medicine vs. We Medicine: Reclaiming Biotechnology for the Common Good. Columbia University Press DOI: 10.7312/dick15974

DIGITALEUROPE. (2020) Two years of GDPR: a report from the digital industry https://www.digitaleurope.org/resources/two-years-of-gdpr-a-report-from-the-digital-industry/#_ftn5)

European Commission (2019a) Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation. European Commission European Commission Directorate-General for Health and Food Safety, Health systems and products, Medical products –quality, safety and innovation, accessible via: https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

European Commission (2019b). Commission Recommendation of 6.2.2019 on a European Electronic Health Record exchange format. COM/2019/800 final. Accessible via https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

European Commission (2020a) A European Strategy for data. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2020/66 final, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN

European Commission (2020b) Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final, accessible via: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act

European Commission (2020c) Guidance from the European Commission on using the public procurement framework in the emergency situation related to the COVID-19 crisis. COM/2020/2078, accessible via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.CI.2020.108.01.0001.01.ENG&toc=OJ:C:2020:108I:FULL

European Data Protection Board (2019a), Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) – 23 January 2019

European Data Protection Board (2019b). Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version 2.0, 4 June 2019

European Data Protection Board (2020a), Guidelines 05/2020 on consent under Regulation 2016/679 – 4 May 2020

European Data Protection Board (2020b), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. 20 October 2020

European Data Protection Board (2020c) EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak – 21 April 2020

European Data Protection Supervisor (2020). A Preliminary Opinion on data protection and scientific research. European Commission. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf. Accessed 20 April 2020.

European Parliamentary Research Service - Scientific Foresight Unit (STOA) (2019). How the General Data Protection Regulation changes the rules for scientific research. PE 634.447 – July 2019 EN. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf

European Patients' Forum (2020) Response to the Public Consultation on the European Strategy on Data

European Patients' Forum (2016) EPF statement, Core Principles from the Patients' Perspective on the Value and Pricing of Innovative Medicines (2016), p.12. https://www.eu-patient.eu/globalassets/policy/epf_pricing_statement_160616.pdf

Flaumenhaft Y, Ben-Assuli O. Personal health records, global policy and regulation review. Health Policy. 2018;122(8):815-826. doi:10.1016/j.healthpol.2018.05.002

Friedman C., Allee N., Delaney B., Flynn A., Silverstein J., Sullivan K., Young K. (2016). The science of Learning Health Systems: Foundations for a new journal. Learning Health Systems. 1. 10.1002/lrh2.10020.

Forcier, M.B., Gallois, H., Mullan, S., Joly, Y. (2019) Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?, Journal of Law and the Biosciences, Volume 6, Issue 1, October 2019, Pages 317–335, https://doi.org/10.1093/jlb/lsz013

Geneviève LD, Martani A, Mallet MC, Wangmo T, Elger BS. Factors influencing harmonized health data collection, sharing and linkage in Denmark and Switzerland: A systematic review. PLoS One. 2019;14(12):e0226015. Published 2019 Dec 12. doi:10.1371/journal.pone.0226015

Goncalves-Ferreira. (2018). HS. Register–An Audit-Trail Tool to Respond to the General Data Protection Regulation (GDPR). Building Continents of Knowledge in Oceans of Data: The Future of Co-Created eHealth, 247, 81.

Groos and Van Veen, E-B. (2020) Anonymised data and the rule of law. Accepted for publication in the European Data Protection Law Review

Grundstrom, C., Väyrynen, K., Iivari, N., Isomursu, M. (2019). Making Sense of the General Data Protection Regulation—FourCategories of Personal Data Access Challenges, Proceedings of the 52nd Hawaii International Conference on System Sciences, p. 5039-5048, https://hdl.handle.net/10125/59941

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, Cham

Hall, A., Finnegan, T., Chowdhury, S., Dent, T., Kroese, M., & Burton, H. (2018). Risk stratification, genomic data and the law. Journal of Community Genetics, 9(3), 195-199.

Hallinan, D. (2020) Broad consent under the GDPR: an optimistic perspective on a bright future. Life Sci Soc Policy 16, 1. https://doi.org/10.1186/s40504-019-0096-3

Hatef E, Rouhizadeh M, Tia I, et al. Assessing the Availability of Data on Social and Behavioral Determinants in Structured and Unstructured Electronic Health Records: A Retrospective Analysis of a Multilevel Health Care System. JMIR Med Inform. 2019;7(3):e13802. Published 2019 Aug 2. doi:10.2196/13802

Hewitt, R. (2011). Biobanking: The foundation of personalised medicine. Current opinion in Oncology 23:112-119)

Hill, E.M., Turner, E.L., Martin, R. M., & Donovan, J. L. (2013). "Let's get the best quality research we can": public awareness and acceptance of consent to use existing data in health research: a systematic review and qualitative study. BMC medical research methodology, 13(1), 72.

Hoeyer K, Bauer S, Pickersgill M. (2019) Datafication and accountability in public health: Introduction to a special issue. Soc Stud Sci. 2019;49(4):459-475. doi:10.1177/0306312719860202

Karampela M., Ouhbi S., & Isomursu M. (2019). Connected Health User Willingness to Share Personal Health Data: Questionnaire Study. Journal of Medical Internet Research, 21(11). doi: 10.2196/14537

Karsten, J., Solbank R. and Helge J. et al. (2011).Ethical endgames: Broad consent for narrow interests; open consent for closed minds Cambridge Quarterly of Healthcare Ethics 20:572-583

Kho M.E., Duffett M., Willison D.J., Cook D.J., Brouwers M.C. (2009). Written informed consent and selection bias in observational studies using medical records: systematic review. Version 2. BMJ.12;338:b866. doi: 10.1136/bmj.b866. PMID: 19282440; PMCID: PMC2769263.

Kirwan, M., Mee, B., Clarke, N. et al. (2020) What GDPR and the Health Research Regulations (HRRs) mean for Ireland: "explicit consent"—a legal analysis. Ir J Med Sci. https://doi.org/10.1007/s11845-020-02331-2

KNAW (2018) Netherlands Code of Conduct Integrity. https://www.knaw.nl/shared/resources/actueel/bestanden/netherlands-code-of-conduct-for-research-integrity-2018-uk

Litton, J.E. (2017). We must urgently clarify data-sharing rules. Nature, 541(7638), 437-437.

Májek O, A Anttila, M Arbyn, E-B van Veen, B Engesæter, S Lönnberg (2018) The legal framework for European cervical cancer screening programmes. The European Journal of Public Health, Vol. 29, No. 2, 345–350

Mee, B., Kirwan, M., Clarke, N. et al. What GDPR and the Health Research Regulations (HRRs) mean for Ireland: a research perspective. Ir J Med Sci (2020).

Menear M., Blanchette M-A., Demers-Payette O., Roy D. (2019). A framework for value-creating learning health systems. Health Research Policy and Systems. 17. 10.1186/s12961-019-0477-3.

Mondschein, C.F. and Monda, C. (2019) The EU's General Data Protection Regulation (GDPR) in a Research Context. P. Chapter 5. In: Kubben et al. (eds.), Fundamentals of Clinical Data Science, https://doi.org/10.1007/978-3-319-99713-1_5

Mourby, M. (2018) et al, 'Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK', (2018) 34(2) Computer Law & Security Review 222

OECD (2017) New Health Technologies—Managing Access, Value and Sustainability' (16 January 2017). https://read.oecd-ilibrary.org/socialissues- migration-health/managing-new-technologies-in-health-care_ 9789264266438-en#page1

OECD (2019a), Recommendation of the Council on Health Data Governance, OECD/LEGAL/0433

OECD (2019b). Using routinely collected data to inform pharmaceutical policies. Analytical Report for OECD and EU countries.

PHG Foundation (2020) The GDPR and genomic data. The impact of the GDPR and DPA 2018 on genomic healthcare and research. Cambridge: PHG Foundation

Phillips M, F Molnár-Gábor, J.O. Korbel, A. Thorogood, Y. Joly, D. Chalmers, D. Townend & B.M. Knoppers (2020) Genomics: data sharing needs an international code of conduct Efforts to protect people's privacy in a massive international cancer project offer lessons for data sharing. Nature 578, 31-33 (2020) doi:10.1038/d41586-020-00082-9 https://www.nature.com/articles/d41586-020-00082-9

Pinto, Eduardo et al. "Identification and Characterization of Inter-Organizational Information Flows in the Portuguese National Health Service." Applied clinical informatics vol. 7,4 1202-1220. 21 Dec. 2016, doi:10.4338/ACI-2016-08-RA-0135

Pormeister, K (2018) Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research. Journal of Law and the Biosciences, Vol 5, 3: 706–723, https://doi.org/10.1093/jlb/lsy023

Porsdam Mann S., Savulescu J., Sahakian B.J. (2016). Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of easy rescue. Philos Trans A Math Phys Eng Sci. Dec 28;374(2083):20160130. doi: 10.1098/rsta.2016.0130. PMID: 28336803; PMCID: PMC5124071.

PWC (2018) Market study on telemedicine. European Commission, Brussels

Rumbold, J. M. M., & Pierscionek, B. (2017). The effect of the general data protection regulation on medical research. Journal of medical Internet research, 19(2), e47.

Schaefer O.O., G. Laurie S., Menon A., Campbelland, A.V., Chuan Voo, T. (2020), Clarifying how to deploy the public interest criterion in consent waivers for health data and tissue research, BMC Medical Ethics, 21:23 https://doi.org/10.1186/s12910-020-00467-5

Schneider, G. (2019) Disentangling health data networks: a critical analysis of Articles 9(2) and 89 GDPR. International Data Privacy Law, Vol. 9, No. 4 p. 253-271

Sethi, N. (2014)i The Promotion of Data Sharing in Pharmacoepidemiology, Eur J Health Law. Eur J Health Law. 2014 Jun; 21(3): 271–296.

Shabani, M.and Borry, P. (2018) Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. European Journal of Human Genetics (2018) 26:149–156. https://doi.org/10.1038/s41431-017-0045-7

Shah N., Coathup, V., Teare H., Forgie I., Giordano G. N., Hansen T. H., Groeneveld L., Hudson M., Pearson E., Ruetten H., & Kaye J. (2019). Sharing data for future research-engaging participants' views about data governance beyond the original project: a DIRECT Study. Genetics in medicine, 21(5), 1131–1138. https://doi.org/10.1038/s41436-018-0299-7

Skovgaard L., Wadmann S., Hoeyer K. (2019). A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. Health Policy 123 (2019) 564–571.

Sousa, M., Ferreira, D.N.G., Pereira, C.S., Bacelar, G., Frade, S., Pestana, O., & Correia, R.C. (2018). OpenEHR based systems and the general data protection regulation (GDPR). Building Continents of Knowledge in Oceans of Data: The Future of Co-Created eHealth.

Stockdale J., Cassell J., & Ford E. (2019). "Giving something back": A systematic review and ethical enquiry into public views on the use of patient data for research in the United Kingdom and the Republic of Ireland. Wellcome open research, 3, 6. https://doi.org/10.12688/wellcomeopenres.13531.2

Timmers, M. Van Veen, E-B. Maas, A.I.R., Kompanje, E.J.O. (2018). Will the Eu Data Protection Regulation 2016/679 Inhibit critical care research? Medical Law Review, vol 27, no. 1, p 59-78

Van Der Wel KA, Östergren O, Lundberg O, et al. (2019) A gold mine, but still no Klondike: Nordic register data in health inequalities in research. Scandinavian Journal of Public Health. P. 1-13.

Van Veen, E.-B. (2018). Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. European Journal of Cancer, 104, 70-80.

Verheij, R.A., Curcin, V., Delaney, B.C., & McGilchrist, M.M. (2018). Possible sources of bias in primary care electronic health record data use and reuse. Journal of medical Internet research, 20(5), e185.

Villani, C., Schoenauer, M., Bonnett, Y., Berthet, C., Comut, A-C., Levin, F. & Rondepierre, B. (2018). For a meaningful Artificial Intelligence: towards a French and European strategy.

Voigt P, von dem Bussche A. (2017) The EU General Data Protection Regulation. A practical guide, Springer

Wallace R, Greene E. (2020) Survey of NCHDs in Ireland to assess their views and opinions in relation to participation in health research and the impact of new Irish data protection regulations. Ir J Med Sci. doi: 10.1007/s11845-020-02185-8)

WHA (2004) 57.13:Genomics and World Health, Fifty Seventh World Health Assembly Resolution ;22nd May 2004

WHO (2002) Genomics and World Health: Report of the Advisory Committee on Health research, Geneva, WHO 2002

ANNEX 1 TABLES LEGAL AND TECHNICAL SURVEY PER MEMBER STATE

Note. In the Tables, the information for the UK is included for reference, but the results of the UK are not included in the totals.

Table A1.1 Please indicate the legal basis under GDPR Articles 6 (1) and derogation basis under Article 9(2) used for processing health data for normal healthcare provision purposes within the context of a patient - healthcare professional relationship. Please note this is for regular data processing, not data processing in an emergency situation, where the vital interest basis may be used. (Q1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
6(1)(a) Consent and 9(2)(a) Consent[1]	12																												
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	9																												
6(1)(c) legal obligation + 9(2)(h) provision of health or social care	21																												
6(1)(e) public interest + 9(2)(h) provision of health or social care	12																												
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	8																												
6(1)(f) legitimate interest + 9(2)(h) provision of health or social care	2																												
Other combination	6																												

Table A1.2 Please indicate if any specific legislation has been adopted in your Member State that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used for planning, management, administration and improvement of the health and care systems entities such as health authorities. (Q17).
If yes, please indicate which combination of legal bases the legislation relies upon when data are used for planning, management, administration and improvement of the health and care systems: (more than one answer may be applicable as different types of organisation might process data for such purposes). (Q17.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	17			■	■	■		■	■	■		■			■	■	■	■		■		■	■		■	■	■		
6(1)(c) legal obligation + 9(2)(h) healthcare	10				■			■	■	■	■	■			■	■									■			■	
6(1)(e) public interest + 9(2)(h) healthcare	13		■		■		■		■		■	■			■	■			■		■							■	■
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	12		■	■	■		■	■		■					■		■		■	■	■						■		■
6(1)(f) legitimate interest + 9(2)(h) healthcare	1							■																					
Other combination*	6				■	■			■	■			■						■										
Not sure	1														■														
No specific legislation	3	■												■										■					

Table A1.3 Please indicate if any specific legislation has been adopted in your Member State that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used for market approval of medicines and devices, such as medicines agencies, EMA, HTA and Notified Bodies.(Q18).
If yes, please indicate which combination of legal bases the legislation relies upon when data are used for market approval of medicines and devices. (More than one answer may be applicable as different types of organisation might process data for such purposes). (Q18.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	7																	1									1		
6(1)(c) legal obligation + 9(2)(h) health or social care	3																												
6(1)(f) legitimate interest + 9(2)(h) health or social care	0																												
6(1)(e) public interest + 9(2)(h) health or social care	3																												
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	4																												
Other combination	3																												
Not sure	0																												
No specific legislation	17																												

Table A1.4 Please indicate if any specific legislation has been adopted in your Member State that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used for monitoring of medical device safety and/or pharmacovigilance. (Q19).
If yes, please indicate which combination of legal bases are relied upon when data are used for monitoring of medical device safety and/or pharmacovigilance. (Q19.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	15																												
6(1)(c) legal obligation + 9(2)(h) healthcare	7																												
6(1)(e) public interest + 9(2)(h) healthcare	5																												
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	6																												
6(1)(f) legitimate interest + 9(2)(h) healthcare	0																												
Other combination	7																												
Not sure	0																												
No specific legislation	9																												

Table A1.5 Please indicate if any specific legislation has been adopted in your Member State that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used for protecting against serious cross-border threats to health. (Q20).
NOTE: some threats are classified as reportable in WHO's International Health Regulations, and therefore intentional law may also apply to this issue (see question 22 below).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	18										N																		
No	8																												
Not sure	1	1																											

Table A1.6 All EU Member States are required to report diagnosis and outcome of the diseases covered by the WHO International Health Regulation, which now also includes COVID-19. Has your Member State enacted any national level specific legislation about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, which are not covered by the IHR? (Q22).
If yes, please indicate which combination of legal bases are relied upon when data are used for protecting against such potentially serious cross-border threats to health. (Q22.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	10																												
6(1)(c) legal obligation + 9(2)(h) healthcare	4																												
6(1)(e) public interest + 9(2)(h) healthcare	2								1*																				
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	8																												
6(1)(f) legitimate interest + 9(2)(h) healthcare	0								1*																				
Other combination	0																												
Not sure	1																												
No specific legislation	12																												

Table A1.7 Most Member States have developed disease registries to record the prevalence and incidence of certain diseases, both common and rare. Does your Member State have specific legislation to address creation of disease registries? (Q23). If yes, please indicate which combination of legal bases are relied upon when data are used in disease registries. (Q23.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	18	■	■	■	■	■		■	■			■			■	■	■				■	■	■	■	■	■	■		■
6(1)(c) legal obligation + 9(2)(h) healthcare	8	■			■	■			■			■			■			■							■				
6(1)(e) public interest + 9(2)(h) healthcare	6				■							■	■		■				■									■	
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	17			■	■	■	■	■	■	■	■	■	■		■	■			■		■			■		■		■	■
6(1)(f) legitimate interest + 9(2)(h) healthcare	1																		■										
Other combination *	5				■	■				■			■								■								
Not sure	0																												
No specific legislation	3										■			■						■									

Table A1.8 Please state if any specific legislation has been adopted that addresses the processing of health data that was originally collected for the purpose of providing care, by third-party public-sector researchers, i.e. by a different controller than that where the treating healthcare professionals were based. (Q26).
If yes, please indicate which legal base in Article 9(2) is relied upon when data are used for research by third-party public-sector researchers. (Q26.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Explicit Consent (Article 9(2)(a))	6																												
Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised	3																												
Broad consent as defined in national legislation, or in accordance with Recital 33	3*																												
Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask for consent) when consent may be waived.	4																												
Article 9(2)(i) public interest in the field of public health	9																												
Article 9(2)(j) research purposes	14																												
Other	1**																												
No specific legislation	12																												

* *In the case of Germany, there is no mention of broad consent in legislation in the sense of legal acts but this should become administrative practice as recently confirmed by a resolution of all supervisory authorities.*
** *In the case of Finland the Act on the Secondary Use of Health and Social Data does not stipulate the legal basis that should be used for further processing in public sector research.*

Table A1.9 Please state if any specific legislation has been adopted that addresses the processing of health data that was originally collected for the purpose of providing care, by third party researchers not in the public sector – i.e. researchers based in not for profit organisations, researchers based in industrial or commercial research organisations and researchers based in other privately funded research organisations. (Q27).
If yes, please indicate which legal base in Article 9(2) is relied upon by such third-party researchers not in the public sector. (Q27.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Explicit Consent (Article 9(2)(a))	7				■		■	■							■				■		■						■		
Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised	3	■				■	■																						
Broad consent as defined in national legislation, or in accordance with Recital 33	3*					■									1						■						■		
Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask for consent) when consent may be waived.	4	■				■	■													■								
Article 9(2)(i) public interest in the field of public health	6	■				■					■				■				■								■		■
Article 9(2)(j) research purposes	13	■			■	■	■	■			■		■		■		■	■	■		■						■		■
Other	1**																										■		
No specific legislation	13		■	■					■	■		■		■		■						■	■	■	■	■		■	

* *In the case of Germany, there is no mention of broad consent in legislation in the sense of legal acts but this should become administrative practice as recently confirmed by a resolution of all supervisory authorities.*
** *In the case of Finland the Act on the Secondary Use of Health and Social Data does not stipulate the legal basis that should be used for further processing in public sector research.*

Table A1.10 GDPR Article 15 stipulates that data subjects (including patients) have a right to access data concerning them. Please indicate the way in which this right may be exercised in your Member State. Note: this question does not relate to research data, see question 34. (Q30).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Through a formal national data access request system established by legislation	9								1*																				
Through a formal regional data access request system established by legislation	0																												
A patient needs to request access from the data controller by direct reference to Article 15 GDPR	20																												
Other	8																												

Table A1.11 Article 17 of the GDPR provides that in certain cases a data subject can ask for data to be erased or have 'the right to be forgotten'. However, Article 17(3) of the GDPR provides that the right shall not apply to the extent that processing is necessary for reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (i) of the GDPR. If not based on article 17 a limitation to the right to be forgotten in healthcare could also be based on article 23. Please indicate if a patient may have medical records deleted in your Member State. (Q32).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes, always	0																												
Yes, but only under certain conditions	9																												
No	16																												
Not sure	2																												

Table A1.12 GDPR Article 20 stipulates that if the data collection was based on consent or on the basis of the creation or execution of a contract, the data subject (patient) has a right to obtain a portable copy of the data. Please indicate which of the following apply in your Member State Note: this question does not relate to research data, see question 34. (Q33).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK}
Through a formal national data portability request system established by legislation	6																												
Through a formal regional data portability request system established by legislation	1																												
A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR	18																												
Patients cannot obtain a portable copy of medical records (Article 20 does not apply because data is not collected on the basis of consent and no sectoral legislation allows this)	4																												

Table A1.13 If you have selected the last option above please describe why Article 20 does not pertain to patient data: (Q33.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Article 20 GDPR does not apply because health data are not collected on the basis of consent	4								1																				
Article 20 GDPR does not apply because data processing is not carried out by automated means (e.g. no Electronic Health record)	1																												
Because legislation pursuant to Article 23(1) has been enacted which limits the scope of the data subject's (patient's) rights.	0																												
Other reason	1																												

Table A1.14 In case the right to data portability is not available to patients in your Member State for one of reasons listed above, do you believe EU level action to support patients access to health data concerning them would be helpful? (Q33.2).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	3								1																				
No	1																												
Not sure	4																												

Table A1.15 Did your country implement the exceptions to the rights of the data subject for research following article 89(2)? (Q34).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	14																												
Yes, but partially, not all	5																												
No	6																												
Not sure	2																												

Table A1.16 Does your country allow that a patient request the removal of specific health data concerning cured diseases (e.g. cancer) from his/her electronic health record? (Q35).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	6																												
No	18																												
Not sure	3																												

Table A1.17 Please indicate below how access to health data for research is organised in your Member State? (Q37).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Application to a local research ethics committee	10																												
Application to a national research ethics committee	9																												
Application to a national data protection agency (DPA)	1																												
Application to a local/national research ethics committee and the DPA	2																												
The data controller provides direct access upon proof of agreement of a research ethics committee or DPA	15																												
The data controller provides direct access without engagement to an ethics committee or DPA	7																												
Application to a centralised data governance and access body (hence other than each data controller / data custodian individually)	7																												
Other	8																												

Table A1.18 What are the functions of the data governance and access body? (multiple choices are possible) (Q38.11).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
To map the sources of information	4		■		■														■								■		■
To make public the sources of information of and their description (what kind of data are available)	6		■		■						■								■							■	■		■
To evaluate the eligibility of the request	7		■		■	■					■				■				■								■		■
To obtain an ethical committee approval	3							■											■								■		
To get in contact with controllers	4		■																■					■			■		■
To do the processing, based on research question and provide the result to requester	5		■		■																			■		■	■		
To request the data from the controllers	5		■								■								■					■			■		
To pseudonymise the data	6				■	■					■								■					■			■		■
To anonymise the data	8	1	■		■	■					■								■					■			■		■
To put the data at the disposal of requester on a secure space	5		■		■	■					■																■		■
To hand out the pseudonymised data to requester	5				■	■					■								■								■		
To hand out the anonymised data to requester	6		■		■	■					■								■								■		
To link health data with other sectors	4		■		■														■								■		■
Other	1										■																		

Table A1.19 If the data governance and access body is able to link health data with other sectors, which sectors are covered? (Q38.12).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Not able to link health data with other sectors	2																												
Health and social	6																												
Education	2																												
Environment	2																												
Connected homes	1																												
Wellness	1																												
Other	1																												

Table A1.20 Do you believe the current legislation in place in your Member State is sufficient to facilitate the free flow of health data between Member States? (Q46).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	6																												
No	17																												
Not sure	4																												

Table A1.21 If no, do you believe an EU level code of conduct could alleviate this situation? (Q46.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	9																												
No	2																												
Not sure	10																												

Table A1.22 Do you believe that the current legislation in place at EU level is sufficient to facilitate the free flow of health data between Member States? (Q47).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	2																												
No	18																												
Not sure	7																												

Table A1.23 If no, do you believe that EU legislation could alleviate this situation? (Q47.1).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	13																												
No	1																												
Not sure	6																												

Table A1.24 If an EU level data governance and access body were to be set up, what form should it take at EU level? (Q54).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
A voluntary network, for primary and secondary use of health data	6																												
Two voluntary networks, for primary and secondary use of health data with some common activities	5																												
A form of public-private partnership	2																												
An EU committee	5																												
An EU agency	10																												
Other	3																												

Table A1.25 Section E also addressed data altruism. Do you believe that a system of data altruism should be set up at EU level? (Q57).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	11																												
No	5																												
Not sure	11																												

Table A1.26 In your Member State are there ICT systems by which healthcare professionals can share the electronic Health Records (EHR) of individual patients with other healthcare professionals? (Q58).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
One national system	20																												
Several national systems	2																												
Several sector specific national systems	4																												
Several sector specific regional systems	6																												
Several systems by separate ICT vendors or service providers	6																												
EHRs are not routinely used for this	1																												
EHRs are used, but no systems are in place to allow for sharing them	4																												
None of the above	0												1																
I don't know	0																												

Table A1.27 In your Member State, is there an ICT system through which patients can access their EHR data? (Q63 and Q 64).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes, this is organised nationally.	22																												
Yes, this is organised regionally.	5																												
Yes, this is organised by individual health services.	1																												
No, there are no such ICT systems	2																												
Other	5																												
I don't know.	0																												
If you answered yes above, do patients have access to the full EHR or just specific parts?																													
Full EHR	13																												
Partial EHR	11																												
I don't know.	0																												

Table A1.28 Are there national or regional interoperability policies regarding the technical standards to be used to ensure that the structure and format of data are interoperable so that such data may be shared between healthcare professionals or incorporated into more than one database for secondary use? (Q70).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
There is one national data interoperability policy	11					■				■		■				■				■	■	■			■	■	■	■	
There are several national data interoperability policies	6	■			■		■	■												■			■						
Each region has one data interoperability policy	2	■								■																			1
Each region has several data interoperability policies	0																												■
There are no national or regional interoperability policies	9		■	■				■	■						■		■	■	■					■					
I don't know	0																												

Table A1.29 Are there national or regional health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely. (Q71).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
There is one national data security policy	16	■	■		■	■	■	■		■		■				■		■		■	■	■			■	■		■	
There are several national data security policies.	4								■		■												■				■		
Each region has one data security policy	1									■																			
Each region has several data security policies	1					■																							■
There are no national or regional data security policies.	4							■							■		■		■										
I don't know	2											■												■					

Table A1.30 Are there national or regional data quality policies regarding the technical standards to be used to ensure the quality of health data for use in EHRs or other digital applications. (Q72).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
There is one national data quality policy which addresses use of standards across all healthcare provider sectors	8																												
There are several national data quality policies which address use of standards for each healthcare provider sector	5																												
Each region has one data quality policies which addresses use of standards across all healthcare provider sectors	1																												
Each region has several data quality policies which address use of standards for each healthcare provider sector	1																												
There are no national or regional data quality policies to ensure use of quality standards for health data	11																												
I don't know	1																												

Table A1.31 In your Member State are entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)? (Q74).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
One national system to share data for secondary use	4																												
Several national systems to share data for secondary use.	5																												
Several sector specific national systems to share data for secondary use.	2																												
Several sector specific regional systems to share data for secondary use.	3																												1
Several systems for sharing data for secondary use, administered by separate ICT vendors or service providers.	2																												
None of the above	16																												
I don't know	0																												

Table A1.32 Please indicate the process used to access data held in EHRs for secondary use (more than one answer may apply) (Q87). Note. This question was only asked for Member State where there is no centralised data access infrastructure

	Total	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Application to the data controller - healthcare provider or healthcare professional	14																												
Application to a research ethics body	6																												
Application to the national Data Protection Authority	1																												
Other	4																												

Table A1.33 Please indicate the types of research that may be conducted using data held in EHRs (more than one answer may apply). (Q89). Please indicate the types of research that may be conducted using data held in disease registries (more than one answer may apply). (Q92). Note. Both questions were only asked for Member State where there is no centralised data access infrastructure

EHR data	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Research for health system monitoring, management and evaluation by a public sector entity	13			■			■	■	■	■		■	■			■		■		■		■	■				■		
Research for medicines and device monitoring and evaluation (incl. pharmacovigilance) by public sector organisations (incl. regulators)	13			■			■	■		■		■	■			■		■		■		■	■				■	■	
Scientific research by not-for - profit academic organisations	13			■			■	■	■	■		■	■			■		■		■			■				■	■	
Commercial scientific organisations (including pharmaceutical and medical technology industry)	10			■			■	■				■	■					■		■			■				■	■	
Any commercial enterprise	4			■				■												■							■		
Other	4														■						■			■		■			

Disease registries	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Research for health system monitoring, management and evaluation by a public sector entity	16			■			■	■	■	■		■	■			■		■		■	■	■	■			■	■	■	
Research for medicines and device monitoring and evaluation (incl. pharmacovigilance) by public sector organisations (incl. regulators)	14			■			■	■		■		■				■		■		■	■	■	■			■	■	■	
Scientific research by not-for - profit academic organisations	15			■			■	■	■	■		■	■			■		■		■	■		■			■	■	■	
Commercial scientific organisations (including pharmaceutical and medical technology industry)	11			■			■	■				■						■		■	■		■			■	■	■	
Any commercial enterprise	7			■				■												■	■					■	■	■	

Table A1.34 Has specific legislation been adopted that addresses the processing of health data that was originally collected for the purpose of providing care, by third party researchers, and if yes, please indicate which legal base in Article 9 (2) is relied upon.

		Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
No specific legislation	Public researchers	12																												
	Non-public researchers	13																												
Explicit Consent (Article 9(2)(a))	Public researchers	6	1	1	1					1	1				1		1						1	1	1	1	1		1	1
	Non-public researchers	7	1	1	1					1	1		1		1		1				1		1	1	1	1	1		1	
Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised	Public researchers	3																												
	Non-public researchers	3																												
Broad consent as defined in national legislation, or in accordance with Recital 33	Public researchers	3*																												
	Non-public researchers	3*														1														
Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask	Public researchers	4																												
	Non-public researchers	4																												
Article 9(2)(i) public interest in the field of public health	Public researchers	9																												
	Non-public researchers	6																												
Article 9(2)(j) research purposes	Public researchers	14																												
	Non-public researchers	13																												
Other	Public researchers	1*																												
	Non-public researchers	1																												

* *In Germany, there is no mention of broad consent in legislation in the sense of legal acts but this should become administrative practice as recently confirmed by a resolution of all supervisory authorities. In Finland the Act on the Secondary Use of Health and Social Data does not stipulate the legal basis that should be used for further processing in public sector research.*

Table A1.35 Article 9(4) of the GDPR states that MS may introduce or maintain further conditions, including limitations with regard to the processing of health data or genetic/biometric data. Please indicate if any such legislation has been adopted in addition to any you have reported above (Q10).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	16																												
No	11																												
Not sure	0																												

Table A1.36 Does your country have any specific regulations for genetic testing, e.g. such testing may only be performed in specially accredited laboratories or centres? (Q3).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	20																												
No	7																												
Not sure	0																												

Table A1.37 Certain devices or apps process data on a platform controlled by the device-maker from which the processed data will be sent to the heath or care professional. Is access to such data on the platform of the device maker assured for patients in your Member State? (Q13).

	Total MS	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	[UK]
Yes	8																												
No	8																												
Not sure	10																												

ANNEX 2 RESULTS STAKEHOLDER ANALYSIS PER TYPE OF RESPONDENT

Table A2.1 Types of stakeholder audiences having responded to the online stakeholder survey

	Frequency	Percent
Individual	62	11%
Patient organisation	80	14%
Health professional	101	18%
Healthcare providers	60	11%
Healthcare insurers	5	1%
Scientific researchers	108	19%
Industry	43	8%
Public Administration/Governmental organisation/MoH	80	14%
Unknown	4	1%
Total	543	100%

Table A2.2 Country of residence of stakeholder audiences having responded to the online stakeholder survey

Country	Frequency	Percent	Country	Frequency	Percent
Austria	14	3%	Latvia	12	2%
Belgium	45	8%	Lithuania	8	2%
Bulgaria	6	1%	Luxembourg	<5	<1%
Croatia	10	2%	Malta	<5	<1%
Cyprus	10	2%	Netherlands	34	6%
Czechia	5	1%	Poland	10	2%
Denmark	16	3%	Portugal	21	4%
Estonia	7	1%	Romania	29	5%
Finland	11	2%	Slovak Republic	<5	<1%
France	36	7%	Slovenia	9	2%
Germany	46	9%	Spain	27	5%
Greece	11	2%	Sweden	8	2%
Hungary	6	1%	United Kingdom	25	5%
Ireland	65	12%	Other non-EU country	28	5%
Italy	38	7%			

TABLES BELONGING TO CHAPTER 3 – FUNCTION 1: STAKEHOLDER VIEWS CONCERNING PROCESSING PERSONAL DATA FOR CARE PURPOSES

Table A2.3 Share of stakeholder agreeing with the following statements, all related to the current legislation and regulations for data sharing

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
The use of different legal bases (e.g. consent, provision of care, public interest) make it difficult for health-related data to be shared for care purposes between EU countries	71%	83%	81%	83%	77%	70%	74%
The current national rules are outdated, given new developments such as personalised medicine, Artificial Intelligence etc.	69%	70%	67%	72%	78%	74%	52%
The current EU rules are outdated, given new developments such as personalised medicine, Artificial Intelligence etc.	66%	61%	67%	60%	68%	70%	46%

Table A2.4 Share of stakeholder agreeing with the following statements, all related to the way in which data sharing for providing care is possible

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
Lack of data portability drives up costs through repeat testing and examination	89%	92%	88%	84%	87%	77%	87%
Lack of data portability slows down time to diagnosis and treatment	89%	93%	89%	85%	86%	74%	85%
Lack of data portability increases the risk of errors	82%	93%	85%	79%	89%	69%	77%
Lack of data portability can limit the rights of Europeans to seek care in another EU country	80%	89%	73%	78%	86%	63%	75%
Lack to data portability can limit the rights to Europeans to work or go on holiday in another EU country	71%	78%	61%	64%	62%	53%	48%
Sharing of data for care provision purposes within my country is very difficult because of low levels of interoperability between health record systems	67%	85%	75%	69%	71%	71%	59%
Sharing of data for care provision purposes with another EU country is very difficult because of low levels of interoperability between health record systems	80%	92%	79%	80%	86%	82%	83%
Sharing of data for care provision purposes within my country is a major privacy risk because of insufficient security measures (including cloud security)	47%	40%	41%	40%	36%	30%	25%
Sharing of data for care provision purposes with another EU country is a major privacy risk because of insufficient security measures (including cloud security)	52%	55%	57%	50%	46%	35%	34%

TABLES BELONGING TO CHAPTER 4 – FUNCTION 2: STAKEHOLDER VIEWS CONCERNING PROCESSING PERSONAL DATA FOR PUBLIC HEALTH PURPOSES

Table 2.5 Share of stakeholder agreeing with the following statements, all related to the way in which data sharing for public health purposes is possible

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
It is easy for the concerned professionals to gain access to health data for public health planning, quality and prevention purposes in my country	34%	38%	25%	34%	35%	16%	48%
Data access for public health purposes is difficult because data sets are scattered over many different providers in my country	69%	82%	65%	81%	71%	55%	64%
Use of data for national level public health purposes is difficult because data are not comparable between different data sets	65%	88%	66%	69%	65%	74%	56%
Use of data for cross-border public health purposes is difficult because data are not comparable between different data sets	73%	86%	76%	77%	69%	77%	81%
The use of different legal bases (eg consent, provision of care, public interest) makes it difficult for health-related data to be shared for public health purposes between EU countries	76%	86%	82%	88%	79%	79%	81%
Different interpretations of whether data are considered anonymised or pseudonymised make it difficult for health-related data to be shared for public health purposes between EU countries	69%	78%	73%	84%	82%	79%	77%

Table A2.6 Share of stakeholder agreeing with the following statements, all related to whether data sharing for public health purposes should be improved

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
Epidemiological institutions should have easier and direct access to health data, in order to ensure their task	74%	82%	78%	82%	79%	61%	86%
Medicine agencies, notified bodies for medical devices or Health Technology Assessment bodies should have easier and direct access to health data, in order to ensure their task	69%	72%	73%	67%	75%	55%	76%
Governance structures, data permit authorities, or single points of contact should ensure that public bodies are allowed to have easier and direct access to health data	77%	67%	71%	79%	68%	39%	72%
The EU should support the processing of health data by epidemiological institutions for the protection against serious cross-border health threats, for example by guidance or legislation	88%	89%	84%	79%	87%	69%	88%
The EU should support the processing of health data by medicine agencies, notified bodies for medical devices or HTA bodies for ensuring high standards of quality and safety, for example by guidance or legislation	82%	81%	78%	76%	82%	64%	83%

Table A2.7 Share of stakeholder agreeing with the following statements, all related to the way in which responses to future communicable disease outbreaks should be improved

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
Ensure that pseudonymised health data on affected citizens can be shared with public health authorities without consent on the basis of public health need for public health purposes	55%	69%	72%	76%	76%	78%	66%
Ensure that only non-identifiable health data on affected citizens can be shared for relevant public health purposes with public health authorities	73%	79%	65%	62%	67%	44%	69%
Facilitate reporting of pseudonymised data of national and regional public health laboratories directly to ECDC without going through a reporting cascade	64%	72%	68%	77%	72%	65%	66%
Facilitate direct reporting of national and regional public health authorities to public health institutions dealing with epidemiological aspects, without going through a reporting cascade	67%	75%	78%	76%	81%	65%	67%
Set up a system at EU level to allow patients to make data available for research without reference to a particular research project (also known as data altruism)	66%	75%	68%	65%	80%	81%	61%
Set up an EU level governance managing the data altruism	68%	76%	65%	68%	69%	83%	53%
Such a data altruism system should also be used for pandemics	69%	71%	72%	65%	71%	87%	56%

TABLES BELONGING TO CHAPTER 5 – FUNCTION 3: STAKEHOLDER VIEWS CONCERNING PROCESSING PERSONAL DATA FOR RESEARCH PURPOSES

Table A2.8 Share of stakeholder agreeing with the following statements, all related to the way in which data sharing for research purposes is possible

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
It is easy to gain access to health data for researchers working in the public domain in my country	43%	15%	24%	25%	28%	26%	47%
It is easy to gain access to health data for research for researchers working in not-for-profit or academic entities in my country	42%	15%	25%	21%	20%	26%	39%
It is easy to gain access to health data for research by commercial entities in my country	29%	9%	5%	11%	21%	9%	15%
It is easy to gain access to health data for research by industry (pharma, medical devices, Artificial Intelligence) in my country	34%	24%	9%	11%	24%	13%	22%
The current data protection rules in my country make data access for research purposes difficult	54%	64%	64%	67%	59%	61%	43%
The time and interaction costs of gaining access to health data for research are high in my country	64%	76%	78%	67%	82%	76%	58%
The financial costs of gaining access to health data for research are high in my country	51%	50%	45%	30%	37%	52%	24%
Rules in my country make access to data for research organisations unnecessary complex	57%	67%	68%	48%	67%	53%	35%
EU rules make access to data for research organisations unnecessary complex	50%	55%	69%	49%	57%	64%	41%

Table A2.9 Share of stakeholder agreeing with the following statements, all related to whether data sharing for research purposes should be improved

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
There is a need for an EU level regulatory and organisational landscape for using health data for research	84%	89%	80%	88%	82%	100%	76%
Different rules for access to data for research purposes for public sector and private sector researchers should apply in my country	59%	66%	47%	41%	56%	21%	52%
The EU should support the processing of health data for scientific or historical research or statistical purposes, for example by guidance or legislation	89%	89%	82%	76%	88%	86%	84%
The EU should support the processing of health data by industry (pharmaceutical, medical devices, Artificial Intelligence) to health data, for example by guidance or legislation	57%	58%	55%	49%	56%	87%	63%
The EU should set up governance structures to support such processing of health data by industry (pharmaceutical, medical devices, Artificial Intelligence)	67%	71%	64%	59%	60%	81%	57%
The EU should promote the use of the same legal base of sharing health data for research purposes	80%	87%	80%	79%	80%	78%	77%
The EU should provide EU level guidance on obtaining consent from patients for sharing data	84%	89%	80%	93%	81%	89%	85%
Different rules for access to data for research purposes for public sector and private sector researchers should apply in my country	61%	64%	47%	42%	59%	18%	53%

TABLES BELONGING TO CHAPTER 6: STAKEHOLDER VIEWS CONCERNING PATIENTS' RIGHTS CONCERNING THE PROCESSING OF PERSONAL DATA

Table A2.10 Share of stakeholder agreeing with the following statements, all related to the current situation regarding patients' rights

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
It is easy for a patient to access his or her medical record in my country	43%	43%	62%	65%	47%	37%	67%
It is easy for a patient in my country to obtain a portable copy of their medical record to take to another healthcare provider in the same country	36%	32%	57%	57%	39%	14%	48%
It is easy for a patient to obtain a portable copy of their medical record to take to another healthcare provider in a different EU country	27%	25%	41%	39%	22%	9%	32%
The medical records in my country are structured around the patient (e.g as personal data space or patient portal)	41%	25%	49%	51%	39%	15%	49%
The current data protection rules in my country do not adequately protect the interest of patients	53%	59%	20%	21%	28%	15%	12%
Having health data in a personal data space /patient portal facilitates the transfers between healthcare providers	66%	65%	80%	71%	73%	69%	80%

Table A2.11 Share of stakeholder agreeing with the following statements, all related to whether patients' rights should be improved

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
Additional measures should be taken at national level to enforce patients' access and control over their own health data and portability of this data	84%	95%	73%	68%	84%	63%	73%
Additional measures should be taken at EU level to enforce patients' access and control over their own health data and portability of this data	80%	93%	79%	78%	81%	80%	74%
The EU should increase awareness of citizens rights on data access to their medical health records/health data under GDPR	90%	93%	76%	78%	80%	72%	86%
The EU should increase awareness of citizens rights on data portability under GDPR (being able to transfer one's personal data to another controller)	88%	93%	80%	87%	80%	75%	81%
The EU should support Member States to reinforce citizens' access, portability and control over their health data, for example by guidance or legislation	86%	97%	75%	82%	86%	81%	79%
The EU should support Member States healthcare providers to ensure the transfer of health data between different healthcare providers and at the request of patients, this to allow patients to provide their health data only once, for example by guidance or legislation	86%	89%	80%	85%	82%	81%	84%
The EU should support Member States to set up personal data spaces or patients' portals centred around patients, for example by guidance or legislation	77%	93%	68%	89%	83%	74%	79%

TABLES BELONGING TO CHAPTER 7: STAKEHOLDER VIEWS CONCERNING GOVERNANCE MODELS AND DATA ALTRUISM

Table A2.12 Share of stakeholder agreeing with the following statements, all related to whether data sharing for scientific research could be improved

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
A single point of contact for the use of health data for research should be supported in my country	80%	81%	78%	70%	81%	67%	80%
Single points of contact should be set up in all Member States, making access to health data for research much simpler	79%	87%	77%	76%	79%	80%	80%
All single points of contact should be linked at EU level, to support pan-European research	76%	85%	79%	78%	80%	83%	78%
One single point of contact should also be set up at EU level, in addition to national ones	72%	77%	73%	60%	71%	65%	70%
The EU should support Member State to put in place structures allowing for secondary use of health data for policy making and research, for example by guidance or legislation	77%	78%	73%	88%	85%	89%	84%

Table A2.13 Share of stakeholder agreeing with the following statements, all related to whether data altruism for scientific research could be improved

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
A system to allow patients to make data available for research without reference to a particular research project (also known as data altruism) should exist in my country	72%	80%	75%	69%	86%	79%	59%
A system to allow patients to make data available for research without reference to a particular research project (also known as data altruism) should exist in my country	70%	76%	71%	67%	83%	77%	65%
A system to allow patients to make data available for research without reference to a particular research project (also known as data altruism) should exist at EU level	67%	77%	71%	71%	80%	80%	61%
The EU should support Member States to set up governance structures for managing data available for research without a reference to a particular research project (data altruism), for example by guidance or legislation	75%	77%	72%	81%	87%	81%	72%
The EU should set up governance structures at EU level for managing data available for research without a reference to a particular research project (data altruism)	76%	80%	73%	73%	81%	78%	64%

TABLES BELONGING TO CHAPTER 8: STAKEHOLDER VIEWS CONCERNING FUTURE ACTIONS

Table A2.14 Share of stakeholder agreeing with the following statements, all related to who should be involved in setting up regulations for the secondary use of data at European level

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
Researchers in the area of public health	90%	95%	82%	91%	95%	87%	90%
Data protection authorities	84%	93%	74%	89%	87%	92%	89%
(Representatives of) healthcare professionals	78%	91%	82%	87%	86%	95%	84%
Patients/patient representatives	86%	96%	72%	75%	87%	92%	83%
Public bodies ensuring the prevention of diseases (such as centres for disease control, national health institutes, institutes monitoring infectious diseases)	79%	89%	73%	82%	87%	87%	87%
Regulators (medicine agencies, Health Technology Assessment and notified bodies, etc.)	78%	83%	75%	73%	81%	89%	87%
International statistics offices (such as Eurostat, WHO, OECD)	76%	85%	75%	74%	82%	71%	81%
National statistics offices	79%	80%	75%	84%	80%	69%	75%
EU policy makers	74%	89%	70%	73%	75%	86%	73%
National policy makers	68%	78%	63%	69%	70%	81%	77%
Biobanks	67%	69%	63%	59%	74%	68%	69%
Commercial parties, such as pharmaceutical industry, manufacturers of wearables, tech industry, insurers	39%	41%	32%	30%	39%	95%	49%

Table A2.15 Share of stakeholder agreeing with the following statements, all related to potential actions that may be taken by the EU for the use of health data for healthcare, policy making and research

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
The EU should provide EU level guidance on anonymising/pseudonymising health data	86%	89%	81%	95%	89%	97%	93%
The EU should support interoperability through the use of open exchange formats / interoperability agreements, for example by guidance or legislation	87%	88%	81%	85%	86%	86%	87%
The EU should promote data quality and reliability through the use of standards	90%	93%	82%	89%	89%	89%	93%
The EU should promote data security through the use of standards health-related cybersecurity standards	88%	94%	80%	91%	88%	87%	91%
The EU should develop minimum datasets for data exchange	75%	88%	78%	91%	75%	71%	82%

Table A2.16 Share of stakeholder agreeing with the following statements, all related to the types of functions an EU level data sharing infrastructure for secondary purposes should have, if it was set up

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
A structure linking all existing health data of different countries to each other	59%	80%	71%	62%	67%	75%	45%
A structure linking the one entry points/data permit authorities of different countries, other research infrastructures and data sources and EU institutions/agencies	56%	71%	69%	67%	71%	80%	59%
A structure intermediating access to health data e.g. a body where a request for access to existing health data can be put forward and managed	57%	71%	65%	71%	76%	75%	57%
A structure managing the health data based on consent of the patients	68%	81%	66%	62%	54%	53%	38%
None of these options, the current set of rules and regulations is sufficient	7%	2%	2%	12%	3%	0%	3%
None of these options, I don't see the value of a common model for health data sharing	7%	3%	1%	6%	5%	3%	5%

Table A2.17 Share of stakeholder agreeing with the following statements, all related to how EU level data sharing infrastructure for secondary purposes should be organised, if it was set up

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
A voluntary network, for both primary and secondary use of health data	30%	38%	37%	22%	30%	31%	32%
Two voluntary networks, one for primary use and one for secondary use of health data with some common activities	31%	31%	22%	19%	28%	27%	32%
A form of public-private partnership	25%	34%	30%	27%	26%	47%	11%
An EU committee	43%	59%	34%	48%	36%	41%	36%
An EU agency	61%	74%	51%	65%	56%	64%	46%
None of these options, because in my view this should not be set up at EU level	6%	7%	7%	0%	4%	9%	8%

Table A2.18 Share of stakeholder agreeing with the following statements, all related to how the governance of an EU level data sharing infrastructure should be assured if it was set up

	individual	patient organisation	health professional	healthcare provider	scientific researchers	industry	public administration/ government org/MoH
A code of conduct put together by representatives of all relevant national authorities	58%	64%	64%	57%	64%	38%	61%
A code of conduct put together by a board of stakeholders	44%	65%	44%	35%	59%	60%	39%
EU level legislation	67%	80%	54%	76%	63%	62%	72%
Other	7%	6%	4%	0%	6%	7%	7%

ANNEX 3 LEGAL AND PRACTICAL SURVEY FOR COUNTRY CORRESPONDENTS

Chafea/2018/Health/03

Specific Contract No 2019 70 01

Experts' Workshop assessing the Member States' rules on health data in the light of GDPR

Survey assessing the Member States' rules on health data in the light of GDPR

Background and purpose of the questionnaire

In line with the communication of the European Commission on "A European strategy for data", the European Commission is considering the potential of the creation of a European Health Data Space (EHDS) to promote health-data exchange and support research on new preventive strategies, as well as on treatments, medicines, medical devices and outcomes. The EHDS should not be seen as a big European 'data lake' but as a system for data exchange and access which is governed by common rules, procedures and technical standards to ensure that health data can be accessed within, and between Member States, with due respect for the rights of individuals as set out in the General Data Protection Regulation (GDPR).

The purpose of this survey is to get as complete a picture as possible of the rules for processing of health data currently in place in each Member State (MS); and to understand whether there is any appetite for the development of new rules and governance systems at EU level to ensure the safe functioning of the EHDS. The survey is split into two parts:

- **Part One** of the survey focuses on legislative measures
- **Part Two** addresses the practical and technical manner in which health data is governed at national level.

Further details on the lay-out of Parts 1 and 2 of the survey are provided at the start of each part.

While the survey is mostly a mapping of the situation as it exists at present, we also value your own interpretation and assessment of the extent to which current tools would be sufficient for the operation of the EHDS and any further developments that would be needed. Accordingly, we ask you to make such comments at the final section of each part.

Thank you for your contributions to this study

On behalf of the EUHealthSupport team,
Johan Hansen, Robert Verheij (Nivel, Netherlands institute for health services research), Petra Wilson (Health Connect Partners), Evert-Ben van Veen (MLC Foundation)

Contact: contact@euhealthsupport.eu

Definitions of terms used in Part One and Part Two

In the survey we use a number of terms which are clarified in greater detail below:

Health data are defined as any personal data generated within healthcare systems, as well as health-related data collected by citizens and patients through wearable devices, apps and self-reported information with the intention to process those data within the healthcare system or for health research. Health data here also includes genetic data and biometric data. Therefore, health data has a wide definition in this survey. This questionnaire is concerned with data that are covered by the GDPR - both personal data as defined in article 4 and sensitive personal data as defined in Article 9. Health and social care are understood in this survey in the sense of article 9(2)(h), to include direct care provision, such as long-term care but does not include in-kind/financial benefits, such as unemployment, guaranteed minimum income etc.

Three broad functions can be distinguished involving processing of health data :

- **Function 1:** Data processing for the purposes of provision of health and social care by health and care providers to the patient concerned. This includes both in-person care and telecare using eHealth or mHealth tools.
- **Function 2**: Data processing for wider public health purposes including planning, management, administration and improvement of health and care systems; prevention or control of communicable diseases; protection against serious threats to health and ensuring high standards of quality and safety of healthcare and of medical products and medical devices.
- **Function 3**: Data processing for scientific or historical research by both public and private sector organisations (third parties, not being the original data controller), including the pharmaceutical and medical technology industries and insurance providers.

Function 1 concerns health data that are collected directly from a patient in the context of health and social care provision for the purpose of providing health or care services to that patient. This is generally referred to as a **primary use**. Such data may need to be shared across EU borders in the case of patients receiving care in a Member State other than their usual Member State of residence. This may be for unplanned care of visitors, unplanned care of temporary residents, planned care in another Member State and care of patients with rare diseases as provided for in **Directive 2011/24/EU on the application of patients' rights in cross-border healthcare**, which includes also the **European Reference Networks on Rare Diseases** as well as under **Regulation (EC) No 883/2004 on the coordination of social security systems.** Such care services may be provided by public or private healthcare providers, and may be financed by public, private or hybrid entities depending on the health and care system of the MS. Note: this includes in-person care as well as telecare using eHealth or mHealth solutions.

Functions 2 and 3 concern the re-use of health data that were collected initially in the context of providing care, but which may later be re-used for another purpose. This is generally referred to as a **secondary use**. Such secondary use may be exercised by **public entities** such as national health systems statutory payers (public bodies of health insurers), public research entities (including universities, public health laboratories), by **regulators** such as medicines agencies and notified bodies as well as by **industry.** The term **industry** includes large and small pharmaceutical and medical technology companies, companies in the insurance and financial services sector, as well as the social media and consumer electronics actors, and the emerging AI industry. Functions 2 and 3 may use data that remain within primary use repositories, such as Electronic Health Records systems, but may also be brought together in other systems such as disease **registries** which collect data to calculate disease incidence

and prevalence at **national or regional level.**

The three functions may take place when the processing falls within one of the exceptions in Article 9(2) GDPR to the general rule in Article 9(1) that health-related data shall not be processed, in most cases such exceptions will apply on the basis of an EU or national law.

For clarity, note that the survey is not concerned with the use of data within clinical trials when the data are collected within a clinical trial in accordance with the Clinical **Trials Regulation**; it is however interested in any legal rules and governance systems that have been adopted to allow further use of data collected for a specific clinical trial in a further trial or for another purpose.

Healthcare: for the sake of simplicity the term 'healthcare' is used to include all types of patient care, even though in some countries some of the care may be labelled social care rather than healthcare. If special rules concerning this social care which is patient care as well, have been adopted in your Member State you can provide comments on this in the comment boxes in this survey.

Healthcare provider is defined in accordance with **Directive 2011/24/EU on the application of patients' rights in cross-border healthcare** to mean "any natural or legal person or any other entity legally providing healthcare on the territory of a Member State."

Healthcare professional is defined in accordance with **Directive 2011/24/EU on the application of patients' rights in cross-border healthcare** to mean a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife, or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment.

Data sharing is used as a generic term by which other parties than the original controller can process the data of that controller, either by performing calculations on the data by the original controller on behalf of the other party and sending the results of those calculations to the other party, or by giving the other party access to the data within the data ecosystem of the controller of by transfer of (excerpts of) the original data to the other party.

Survey Part One: Legal analysis of the governance of health data processing at national level

Part 1 of this survey is divided into 5 sections.

- Section A - concerns the legal framework for processing data for patient care (function 1).
- Section B - concerns the legal framework for processing patient data for planning, management, administration and improvement of the health and care systems; ensuring safety of medicines and medical devices and protection against serious cross-border threats to health (function 2)**.**
- Section C - concerns the legal framework for processing patient data for scientific or historical research by both public and private sector organisations (function 3).
- Section D – concerns the way in which patients are supported in exercising the rights with respect to data as provided for in GDPR.
- Section E - concerns other legal and regulatory issues addressing the use of health data for research purposes.
- Section F – provides the opportunity for you to share your thoughts on future needs for regulating access to health data.

Section A: Questions concerning Function 1 (patient care)

Regulations concerning health data processing and sharing in Function 1 (the primary function of health or care provision). This section includes 16 questions**,** questions 1-10 relate to in-person care, while questions 11-16 relate to care provided at a distance through digital health solutions. *Note: for the sake of simplicity the term 'healthcare' is used to include all types of patient care, even though in some countries some of the care may be labelled social care rather than healthcare. If special rules concerning this social care which is patient care as well, have been adopted in your MS please provide comment on this, and any other significant issues, in the comment boxes.*

1. Please indicate the legal basis under GDPR Articles 6 (1) and derogation basis under Article 9(2) used for **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship. Please note this is for regular data processing, not data processing in an emergency situation, where the vital interest basis may be used.

   ☐ 6(1)(a) Consent and 9(2)(a) Consent[33]
   ☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
   ☐ 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
   ☐ 6(1)(e) public interest + 9(2)(h) provision of health or social care
   ☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
   ☐ 6(1)(f) legitimate interest + 9(2)(h) provision of health or social care
   ☐ Other combination - please specify
   ☐ Not sure

[33] NB: for the avoidance of doubt, consent here means consent in the sense of article 4.11 and article 7 GDPR. It should be distinguished from consent as a basic principle in medical law before diagnostic or treatment procedures may start.

2. Please name and describe any healthcare sector specific legislation which regulates the way in which **health or care providers and health or care professionals** process health data for direct in person care of the data subject.

3. Does your country have any specific regulations for genetic testing, e.g. such testing may only be performed in specially accredited laboratories or centres?

☐ Yes

☐ No

☐ Not sure

3.1 If yes, please specify…

3.2 If yes, do you believe that this special regime can accommodate genetic testing in the context of personalised medicine (e.g. for certain biomarkers which a specific drug will target)

4. Under what conditions **are healthcare providers or professionals allowed to share health data** with another healthcare provider or healthcare professional so that the other professional may provide care?

☐ 6(1)(a) Consent and 9(2)(a) Consent

☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

☐ 6(1)(c) legal obligation + 9(2)(h) provision of health or social care

☐ 6(1)(e) public interest + 9(2)(h) provision of health or social care

☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

☐ 6(1)(f) legitimate interest + 9(2)(h) provision of health or social car

☐ Other combination - please specify

☐ Not sure

5. Please name and describe any **healthcare sector specific** legislation which regulates the way in which healthcare providers and healthcare professionals may share health data among themselves for healthcare provision purposes.

5.1 Please indicate if any legislation exists that allows patient to block such sharing in the healthcare sector and if so, under what conditions.

6. If in your MS the regulations referred to the questions 1 and 2 differ **from region to region**, does this hamper the exchange of patient data between the regions? Please describe the situation and its impact.

7. If the regulations referred to the questions 1 and 2 were to differ **between MS**, do you believe that this would hamper cross-border exchange of patient data? Please set out your opinion in detail.

8. Some Member States have adopted legislation or rules that facilitates data from the Electronic Health Record (EHR) to be exported into a "personal health environment (PHE)"[34] or another form of citizen/patient-controlled record. Please indicate if this exists in your Member State. More than one answer may be applicable:
   - ☐ Yes – regulation/legislation is in place that facilitates export of EHR data to a personal health data environment
   - ☐ Not yet - but legislation is currently being developed that will facilitate export of EHR data to a personal health data environment
   - ☐ No - there is no formal regulation/legislation for export of data to a PHE
   - ☐ Not sure

   8.1 If yes, please name and describe the legislation/rules, including any specific governance rules and the functions of the institutions dealing with this. If no, please describe whether there has been any discussion in your country about this issue.

9. Many healthcare providers use external data processors as defined in Article 4(8) GDPR. Does your MS have specific rules (in addition to Article 28 GDPR) about the employment of data processors for health data?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

   9.1 If yes, please name and describe any legislation or rules that address the use of health data processors for health data.

[34] For an example see: https://www.medmij.nl/en/

10. Article 9(4) of the GDPR states that MS may introduce or maintain further conditions, including limitations with regard to the processing of health data or genetic/biometric data. Please indicate if any such legislation has been adopted in addition to any you have reported above.

☐ Yes

☐ No

☐ Not sure

10.1 If yes, please name and describe the legislation, including relevant details on the kind of health data it concerns (e.g. genetic data).

Regulations concerning health data processing and sharing in <u>Function 1</u> (the primary function of health or care provision) using telecare, telemonitoring, mHealth or other digital health solutions

Many MS have implemented digital health solutions such as remote monitoring by apps and devices teleconsultation by video, and other digital health tools. The questions below concern the way in which GDPR has been interpreted with respect to digital health in your MS.

11. Please state if any specific legislation has been adopted in your MS that addresses the processing of health data **for providing digital health services** (e.g. telehealth and m-health).

☐ Yes

☐ No

☐ Not sure

11.1 Please name and describe such specific legislation

12. In some MS a healthcare professional will **prescribe the use of an app or a device which collects patient data.** This may include apps which require the patient to record data (food intake, sleep, mood, etc.) or apps and devices which automatically record data (steps, heart rate, blood glucose, etc.). The patient's consent to the use of such an app or device will be based on national level medical law, however, the processing of the data from such apps or devices must also be legitimated under the GDPR.
Please indicate which legal basis is used for processing app or device derived data in the healthcare setting.

☐ 6(1)(a) Consent and 9(2)(a) Consent

☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

☐ 6(1)(c) legal obligation + 9(2)(h) health or social care

☐ 6(1)(e) public interest + 9(2)(h) health or social care

☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

☐ 6(1)(f) legitimate interest + 9(2)(h) health or social care

☐ Other combination - please specify

☐ Not sure

13. Certain devices or apps process data on a platform controlled by the device-maker from which the processed data will be sent to the heath or care professional. Is access to such data on the platform of the device maker assured for patients in your Member State?

☐ Yes

☐ No

☐ Not sure

14. If you have responded positively to any of the questions 11-13 please name and describe any sectoral legislation in place that addresses these issues.

15. Are you aware of any issues relating to GDPR that impact on the provision of digital health services?

☐ Yes

☐ No

☐ Not sure

15.1 If yes, does it impact mostly the provision of digital health services at national or cross-border level, for instance by not sharing telemedicine data between different healthcare providers or MS?

☐ National

☐ Cross-border

☐ Both

Please provide further explanations

16. Are you aware of any obstacles to the transfer of data from apps/telehealth between Member States, if the legal basis for processing the data at the national level are different?

☐ Yes

☐ No

☐ Not sure

16.1 If you have answered yes above, please describe the obstacles and if any processes exist to overcome them or what measures you would consider necessary in order to overcome them?

Section B Questions related to Function 2 (secondary use for planning, management health systems improvement)

Regulations concerning data processing and sharing in Function 2 (planning, management, administration and improvement of the health and care systems; ensuring safety of medicines and medical devices; protection against serious cross-border threats to health).

Article 9(1) of the GDPR notes that in general processing of data concerning health or genetic data shall be prohibited, but provides in 9(2) that this prohibition will not apply if the data subject has given explicit consent or, in the case of health related data, that additional national level legislation has been adopted that addresses the processing of health data for the purposes **of providing healthcare (9(2)(h)) or for public health reasons (9(2)(i)).** Through the following questions we would like to learn more about whether such special legislation has been adopted, and if not how secondary use of data has been managed.

This section contains questions about 5 types of such secondary use:

- A number of questions look at **planning, management, administration and improvement of the health and care systems**
- A number of questions look at **market approval of medical device and medicines**
- A number of questions look at **medical device monitoring and pharmacovigilance (PMS)**
- A number of questions look at **protection against serious cross-border threats to health**
- A number of questions look at **disease registries**

If all aspects are addressed in the same way in your Member State, please feel free to answer only question 17. If not please answer all questions.

Questions relating to planning, management and administration in healthcare systems

17. Please indicate if any specific legislation has been adopted in your MS that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used **planning, management, administration and improvement of the health and care systems** entities such as health authorities.

☐ Yes

☐ No

☐ Not sure

17.1 If yes, please indicate which combination of legal bases the legislation relies upon when data are used for **planning, management, administration and improvement of the health and care systems:** *(more than one answer may be applicable as different types of organisation might process data for such purposes)*

☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

☐ 6(1)(c) legal obligation + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

☐ 6(1)(f) legitimate interest + 9(2)(h) healthcare

☐ Other combination - please specify

☐ Not sure

17.2 If yes, please name and describe such specific legislation:

17.3 If the legal basis is consent, please indicate how the completeness of the data available for the **monitoring the quality and planning of the healthcare system** is addressed.

17.4 If the legal basis is not consent (i.e. it is sectoral legislation based on paragraphs (h) or (i)) does the sectoral legislation allow for the patient to object to this data processing?

☐ No

☐ Yes

☐ It will depend on what data processing

17.5 If you have ticked 'yes' or 'it depends' above, please describe below how this operates.

17.6 If no specific legislation has been adopted, please indicate if any policy statement has been adopted at national level in your MS that states that only explicit consent as provided for in 9(2)(a) can permit the processing of health data for **planning, management, administration and improvement of the health and care systems**:

☐ Yes, statement states that explicit consent is the only bases for re-use of data for function 2

☐ Not sure

17.7 If yes, please specify about the nature of that statement (from government, the DPA etc.)

Questions relating to market approval of medicines and devices

18. Please indicate if any specific legislation has been adopted in your MS that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used for **market approval of medicines and devices**, such as medicines agencies, EMA, HTA and Notified Bodies.

☐ Yes

☐ No

☐ Not sure

18.1 If yes, please indicate which combination of legal bases the legislation relies upon when data are used for **market approval of medicines and devices.** *(More than one answer may be applicable as different types of organisation might process data for such purposes)***.**

☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

☐ 6(1)(c) legal obligation + 9(2)(h) health or social care

☐ 6(1)(f) legitimate interest + 9(2)(h) health or social care

☐ 6(1)(e) public interest + 9(2)(h) health or social care

☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

☐ Other combination - please specify

☐ Not sure

18.2 If yes, please name and describe such specific legislation

18.3 If the legal basis is consent, please indicate how the completeness and accuracy of the data used for **monitoring the market approval of medicines and devices** is assured.

18.4 If the legal basis is not consent (i.e. it is sectoral legislation based on paragraphs (h) or (i)) does the sectoral legislation allow for the data subject to object to this data processing?

☐Yes

☐No

☐It will depend on what data processing

18.5 If you have ticked 'yes' or 'it depends' above, please describe below how this operates.

18.6 If no specific legislation has been adopted, please indicate if any policy statement has been adopted at national level in your MS that states that only explicit consent as provided for in 9(2)(a) can permit the processing of health data for market approval of medicines and devices

☐ Yes, statement explicitly states that consent is the only bases for re-use of data for function 2

☐ Not sure

18.7 If yes, please specify about the nature of that statement (from government, the DPA etc.)

Questions relating to device safety and/or pharmacovigilance

19. Please indicate if any specific legislation has been adopted in your MS that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used for **monitoring of medical device safety and/or pharmacovigilance**.

☐ Yes

☐ No

☐ Not sure

19.1 If yes, please indicate which combination of legal bases are relied upon when data are used for monitoring of medical device safety and/or pharmacovigilance

☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

☐ 6(1)(c) legal obligation + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

☐ 6(1)(f) legitimate interest + 9(2)(h) healthcare

☐ Other combination - please specify

☐ Not sure

19.2 If yes, please name and describe such specific legislation

19.3 If the legal basis is consent, please indicate how the completeness of the data used for **monitoring of medical device safety and/or pharmacovigilance** is addressed

19.4 If the legal basis is not consent (i.e. it is sectoral legislation based on paragraphs (h) or (i)) does the sectoral legislation allow for the data subject to object to this data processing?

☐ Yes

☐ No

☐ It will depend on what data processing

19.5 If you have ticked 'yes' or 'it depends' above, please describe below how this operates.

19.6 If no specific legislation has been adopted, please indicate if any policy statement has been adopted at national level in your MS that states that only explicit consent as provided for in 9(2)(a) can permit the processing of health data for **monitoring of medical device safety and/or pharmacovigilance**

☐ Yes, statement explicitly states that consent is the only bases for re-use of data for function 2

☐ Not sure

19.7 If yes, please specify about the nature of that statement (from government, the DPA etc.)

Questions relating to cross border health threats.

20. Please indicate if any specific legislation has been adopted in your MS that addresses the processing of health data that was originally collected for the purpose of providing care to allow it to be used for **protecting against serious cross-border threats to health.**
*NOTE: some threats are classified as reportable in **WHO's International Health Regulations**, and therefore intentional law may also apply to this issue (see question 22 below)*

☐ Yes

☐ No

☐ Not sure

Please name and describe such specific legislation:

21. Under legislation in your MS, is it possible that data are transmitted from the laboratories directly to institutions dealing with communicable diseases/ECDC, without going through a reporting cascade?

☐ Yes

☐ No

☐ Not sure

21.1 If yes, please describe the legislation or guidance that allows for such direct reporting.

22. All EU MS are required to report diagnosis and outcome of the diseases covered by the WHO International Health Regulation, which now also includes COVID-19. Has your MS enacted any national level specific legislation about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, which are not covered by the IHR?

☐ Yes

☐ No

☐ Not sure

22.1 If yes, please indicate which combination of legal bases are relied upon when data are used for **protecting against such potentially serious cross-border threats to health**.

☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

☐ 6(1)(c) legal obligation + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

☐ 6(1)(f) legitimate interest + 9(2)(h) healthcare

☐ Other combination - please specify

☐ Not sure

22.2 If the legal basis is consent, please indicate how the completeness of the data used for **protecting against serious cross-border threats to health not covered by the IHR** is addressed

22.3 If the legal basis is not consent (i.e. it is sectoral legislation based on paragraphs (h) or (i)), does the sectoral legislation allow for the data subject to object to this data processing?

☐ Yes

☐ No

☐ It will depend on what data processing

22.4 If you have ticked 'yes' or 'it depends' above, please describe below how this operates.

22.5 If no specific legislation has been adopted, please indicate if any policy statement adopted in your MS at national level that states that only explicit consent as provided for in 9(2)(a) can permit the processing of health data for **protecting against serious cross-border threats to health not covered by the IHR**.

☐ Yes, statement explicitly states that consent is the only bases for re-use of data for function 2

☐ Not sure

22.6 If yes, please specify about the nature of that statement (from government, the DPA etc.)

Questions relating to disease registries.

23. Most MS have developed **disease registries** to record the prevalence and incidence of certain diseases, both common and rare. Does your Member State have specific legislation to address creation of **disease registries?**

☐ Yes

☐ No

☐ Not sure

23.1 If yes, please indicate which combination of legal bases are relied upon when data are used in disease registries

☐ 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

☐ 6(1)(c) legal obligation + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(h) healthcare

☐ 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

☐ 6(1)(f) legitimate interest + 9(2)(h) healthcare

☐ Other combination - please specify

☐ Not sure

23.2 If the legal basis is consent, please indicate how the completeness of the data in **disease registries** is addressed

23.3 If the legal basis is not consent (i.e. it is sectoral legislation based on paragraphs (h) or (i)), does the sectoral legislation allow for the data subject to object to this data processing?

☐ Yes

☐ No

☐ It will depend on what data processing

23.4 If you have ticked 'yes' or 'it depends' above, please describe below how this operates.

23.5 Please provide further detail below on who, according to the legislation in your MS, may legally be given **access to data held in the disease registry.** (multiple answers are possible)

☐ A healthcare professional may be given access to the data that he or she has submitted to the registry

☐ A Healthcare provider may be given access to the data concerning any patients in its geographical coverage or jurisdiction.

☐ A patient may be given access to any data concerning themselves

☐ A patient is in principle granted access but given the pseudonymised nature of the data concerned, article 11 GDPR will apply and the patient is referred back to his or her healthcare provider

☐ Payers of the healthcare systems (governmental bodies, statutory health insurers)may be given access to the data concerning patients in their coverage or jurisdiction

☐ Other national governmental agencies

☐ International agencies such as EMA or ECDC
☐ Patient organisations
☐ Public sector researchers
☐ Private researchers
☐ Private sector organisations
☐ Others, please specify

23.6 If no specific legislation has been adopted, please indicate if any policy statement adopted in your MS at national level that states that only explicit consent as provided for in 9(2)(a) can permit the processing of health data for creating **disease registries**
☐ Explicit consent is the bases for re-use of data for function 2
☐ Not sure

Section C. Questions concerning Function 3 (secondary use for scientific or historical research)

Regulations concerning health data processing and sharing in Function 3 (scientific or historical research within both public and private sector)

Article 9(1) notes that in general processing of data concerning health or genetic data shall be prohibited, but provides in 9(2) that this prohibition will not apply if the data subject has given explicit consent or, in the case of health related data, that additional national level legislation has been adopted that addresses the processing of health data for the purposes of **general public interest or research (9(2)(j).** Through the following questions we would like to learn more about whether such special legislation has been adopted, and if not how secondary use of data is managed. We are also interested to learn about any **technical and organisational security measures required under Article 89(1)** that have been adopted to allow secondary use of data for research purposes.

This section addresses different types of research:

- A number of questions are **general questions about legislation which addresses the re-use of health data for research**
- A number of questions concern research conducted by the **healthcare professional who originally collected** the data for the purposes of treating the patient, this may also be a healthcare professionals covered by the same data controller (i.e. working for the same healthcare provider)
- A number of questions concern research conducted by or by **third party researchers**, which may include public sector or publicly funded researchers, researchers based in not for profit organisations and researchers based in industry or commercial research organisations other privately funded research organisations.
- A number of questions concerns research by any type of organisation on **genetic data**

24. Article 5.1(b) states that data may generally not be further processed for purposes that are not compatible with the purposes stated to the data subject at the time of data collection. It notes however that further processing for scientific or historical research purposes is not to be considered incompatible with the initial purpose if suitable safeguards in accordance with Article 89(1) of the GDPR are adopted.

Has your MS adopted sectoral legislation or authoritative guidance which further specifies the application of this article in the context of health research?

☐ Yes

☐ No

☐ Not sure

24.1 If yes, please indicate if any of the following issues are addressed specifically in that legislation, and provide further details in the box below? (multiple choices are possible)

☐ Scientific research by public sector organisations

☐ Scientific research by private sector organisations

☐ Research for development of national statistics

☐ Research for authorities' planning

☐ Other, please explain

24.2 Please provide a description of the issues covered in the legislation

25. Please state if any specific legislation has been adopted that addresses the processing of health data that was originally collected for the purpose of providing care **by the healthcare professional who originally collected the data for the purposes of treating the patient, or by other healthcare professionals working for the same healthcare provider**?

☐ Yes

☐ No

☐ Not sure

25.1 If yes, please indicate which legal base in Article 9 (2) is relied upon in the legislation when data are used for research **by the healthcare professionals (the treatment team) who originally collected the data for the purposes of treating the patient, or by other healthcare professionals working for the same healthcare provider.**

☐ Explicit Consent (Article 9(2)(a))

☐ Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised

☐ Broad consent as defined in national legislation, or in accordance with Recital 33

☐ Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask for consent) when consent may be waived.

☐ Article 9(2)(i) public interest in the field of public health

☐ Article 9(2)(j) research purposes

☐ Other

25.2 Please specify and indicate whether a difference is made here between the treatment team and others working at the same healthcare provider (= controller in the sense of the GDPR)

26. Please state if any specific legislation has been adopted that addresses the processing of health data that was originally collected for the purpose of providing care**, by third-party public-sector researchers**, i.e. by a different controller than that where the treating healthcare professionals were based.

☐ Yes

☐ No

☐ Not sure

26.1 If yes, please indicate which legal base in Article 9(2) is relied upon **when data are used for research by third-party public-sector researchers**

☐ Explicit Consent (Article 9(2)(a))

☐ Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised

☐ Broad consent as defined in national legislation, or in accordance with Recital 33

☐ Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask for consent) when consent may be waived.

☐ Article 9(2)(i) public interest in the field of public health

☐ Article 9(2)(j) research purposes

☐ Other

26.2 Please specify

27. Please state if any specific legislation has been adopted that addresses the processing of health data that was originally collected for the purpose of providing care**, by third party researchers not in the public sector – i.e. researchers based in not for profit organisations, researchers based in industrial or commercial research organisations and researchers based in other privately funded research organisations.**

☐ Yes

☐ No

☐ Not sure

27.1 If yes, please indicate which legal base in Article 9(2) is relied upon **by such third-party researchers not in the public sector.**

- ☐ Explicit Consent (Article 9(2)(a))
- ☐ Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised
- ☐ Broad consent as defined in national legislation, or in accordance with Recital 33
- ☐ Explicit consent is the default but the legislation states certain circumstances (such as that it is not possible to ask for consent) when consent may be waived.
- ☐ Article 9(2)(i) public interest in the field of public health
- ☐ Article 9(2)(j) research purposes
- ☐ Other

27.2 Please indicate if the legislation **differentiates between not for profit researchers and for profit researchers.**

- ☐ Yes
- ☐ No
- ☐ Not sure

27.3 If yes please indicate if the legislation excludes access for any of the following researchers:

- ☐ Researchers in or working for public health insurance companies (e.g. mutual)
- ☐ Researchers in or working for private health insurance companies
- ☐ Employers or researchers working for employers
- ☐ Researchers in or for pharmaceutical companies
- ☐ Researchers in or for medical device companies
- ☐ Not sure

27.4 Please describe the legislation in as much detail as possible.

28. Has any special legislation been adopted in your MS for research with **genetic data?**

- ☐ Yes
- ☐ No
- ☐ Not sure

28.1 Does this legislation differ from the legal grounds to process data for research as described in questions 24-26 ?

- ☐ Yes
- ☐ No
- ☐ Not sure

28.2 If yes, please specify

28.3 If yes, does the legislation **differentiate between not for profit researchers and for profit researchers**

- ☐ Yes
- ☐ No
- ☐ Not sure

28.4 If yes, please indicate if the legislation excludes access to genetic data for any of the following researchers:

- ☐ Researchers in or working for public health insurance companies (e.g. mutual)
- ☐ Researchers in or working for private health insurance companies
- ☐ Employers or researchers working for employers
- ☐ Researchers in or for pharmaceutical companies
- ☐ Researchers in or for medical device companies
- ☐ Not sure

28.5 Please provide further clarification on this legislation

Section D – concerns questions regarding patient rights

The GDPR gives data subjects (patients) many rights, including the right to be informed about the purpose of data processing, access to data concerning them, and in certain situations the right to erasure and portability. In these questions we would like to learn more about how those rights are addressed in the context of health-related data in your MS.

29. Has your MS adopted legislation that further clarifies or details the requirements set out in the GDPR about the transparency and accountability of researchers or research projects (including the rights in articles 13 and 14 GDPR)?

- ☐ Yes
- ☐ No
- ☐ Not sure

29.1 If yes, please name and describe the legislation

30. GDPR Article 15 stipulates that data subjects (including patients) have a right to access data concerning them. Please indicate the way in which this right may be exercised in your MS. *Note: this question does not relate to research data, see question 34.*

- ☐ Through a formal national data access request system established by legislation
- ☐ Through a formal regional data access request system established by legislation

☐ A patient needs to request access from the data controller by direct reference to Article 15 GDPR

☐ Other, please specify

30.1 If health data access legislation has been adopted, please name and describe the legislation.

31. Article 16 of the GDPR requires that a data subject shall have the right to rectify any inaccurate data concerning him or her. Please indicate how this operates in your MS. *Note: this question does not relate to research data, see question 34.*

☐ Through a formal national data rectification request system established by legislation

☐ Through a formal regional data rectification request system established by legislation

☐ A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR

☐ The right to rectification is restricted based on sectoral legislation adopted in accordance with Article 23(1)

31.1 If you have selected the last option above, please describe the legislation noting in particular if the patient has a legal right to add a personal note regarding to the error he or she believes to exist.

32. Article 17 of the GDPR provides that in certain cases a data subject can ask for data to be erased or have 'the right to be forgotten'. However, Article 17(3) of the GDPR provides that the right shall not apply to the extent that processing is necessary for reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (i) of the GDPR. If not based on article 17 a limitation to the right to be forgotten in healthcare could also be based on article 23. Please indicate if a patient may have medical records deleted in your MS

☐ Yes, always

☐ Yes, but only under certain conditions

☐ No

☐ Not sure

32.1 Please name and describe any sectoral legislation in place to address this issue.

33. GDPR Article 20 stipulates that if the data collection was based on consent or on the basis of the creation or execution of a contract, the data subject (patient) has a right to obtain a

portable copy of the data. Please indicate which of the following apply in your MS *Note: this question does not relate to research data, see question 34.*

- ☐ through a formal national data portability request system established by legislation
- ☐ through a formal regional data portability request system established by legislation
- ☐ A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR
- ☐ Patients cannot obtain a portable copy of medical records (Article 20 does not apply because data is not collected on the basis of consent and no sectoral legislation allows this)

33.1 If you have selected the last option above please describe why Article 20 does not pertain to patient data:

- ☐ Article 20 GDPR does not apply because health data are not collected on the basis of consent
- ☐ Article 20 GDPR does not apply because data processing is not carried out by automated means (e.g. no Electronic Health record)
- ☐ Because legislation pursuant to Article 23(1) has been enacted which limits the scope of the data subject's (patient's) rights.
- ☐ Other reason, please specify:

33.2 In case the right to data portability is not available to patients in your MS for one of reasons listed above, do you believe EU level action to support patients access to health data concerning them would be helpful?

- ☐ Yes
- ☐ No
- ☐ Not sure

33.3 If yes, please describe the sort of action that could be helpful

34. Did your country implement the exceptions to the rights of the data subject for research following article 89(2)?

- ☐ Yes
- ☐ Yes, but partially, not all
- ☐ No
- ☐ Not sure

34.1 If yes, or partially yes, please specify

35. Does your country allow that a patient request the removal of specific health data concerning cured diseases (e.g. cancer) from his/her electronic health record?

☐ Yes
☐ No
☐ Not sure

35.1 If yes, please describe the conditions

36. Does your country allow that such a request is rejected by the competent authority or body?
☐ Yes
☐ No
☐ Not sure

36.1 If yes, please describe the competent authority and the conditions

Section E - concerns legal or regulatory mechanisms which address the use of health data for research purposes.

In this section we are keen to learn more about the wider legal framework in your MS which defines how health data may be used for research.

- A number of questions address **data access**, including data access agencies and research hubs
- A number of questions addresses **data altruism**, also referred to as data donation.
- A number of questions address **data quality and origin**

Data Access

37. Please indicate below how access to health data for research is organised in your MS? (Multiple answers are possible)
☐ Application to a local research ethics committee
☐ Application to a national research ethics committee
☐ Application to a national data protection agency (DPA)
☐ Application to a local/national research ethics committee and the DPA
☐ The data controller provides direct access upon proof of agreement of a research ethics committee or DPA

☐ The data controller provides direct access without engagement to an ethics committee or DPA

☐ Application to a centralised data governance and access body (hence other than each data controller / data custodian individually)

☐ Other – please specify below

37.1 If you have answered positively to 'application to' , please specify whether there are by-laws or other regulations that have instituted exemptions to the principle that the research must first be submitted to that body, such as that the application is not necessary when the data have been pseudonymised.

37.2 Is there a review mechanism for decisions made by the body or bodies you have selected above

☐ Yes

☐ No

☐ Not sure

37.3 If yes, please explain

38. If you have replied **'centralised data governance and access body'** in question 37, please provide further detail on the agency by answering the question below and providing details in the box.

If your MS does not have such a body please move to question 39

38.1 A data governance and access body has been created in my MS at:

☐ National level

☐ Regional level

☐ Sub regional level

☐ Other - please specify below

38.2 The data governance and access body provides access for:

☐ All researchers

☐ Public sector researchers only

☐ Other categories – please specify below

38.3 The data governance and access body provides a single point of entry for researches to access data:

☐ Yes

☐ No

☐ Not sure

38.4 The data governance and access body hosts data:

☐ Yes

☐ No

☐ Not sure

38.5 The data governance and access body provides access to data that remains stored with the original data controller:

☐ Yes

☐ No

☐ Not sure

38.6 How is the data governance and access body organised?

☐ Public institution

☐ Private institution

☐ Public-private partnership

Please provide more information about each type of organisation…

38.7 Data access requests from researchers in other EU countries can be submitted to the data governance and access body in your MS:

☐ Yes

☐ No

☐ Not sure

38.8 If yes, please explain any limitations or criteria that are applicable

38.9 Is there a review mechanism for decisions made by the data governance and access body in your MS?

☐ Yes

☐ No

☐ Not sure

38.10 If yes, please explain

38.11 What are the functions of the data governance and access body? (multiple choices are possible)

- ☐ To map the sources of information
- ☐ To make public the sources of information of and their description (what kind of data are available)
- ☐ To evaluate the eligibility of the request
- ☐ To obtain an ethical committee approval
- ☐ To get in contact with controllers
- ☐ To do the processing, based on research question and provide the result to requester
- ☐ To request the data from the controllers
- ☐ To pseudonymise the data
- ☐ To anonymise the data
- ☐ To put the data at the disposal of requester on a secure space
- ☐ To hand out the pseudonymised data to requester
- ☐ To hand out the anonymised data to requester
- ☐ To link health data with other sectors
- ☐ Other – please specify

38.12 If the data governance and access body is able to link health data with other sectors, which sectors are covered?

- ☐ Not able to link health data with other sectors
- ☐ Health and social
- ☐ Education
- ☐ Environment
- ☐ Connected homes
- ☐ Wellness
- ☐ Other – please specify

Data Altruism

39. Some MS have put in place system to foster data altruism (sometime referred to also as data donation), through which patients can make available data concerning themselves for researchers to use.
Has any such system been adopted in your MS that established a possibility for provide their data to be used by researchers without reference to a particular research project?

- ☐ Yes
- ☐ No
- ☐ Not sure

39.1 If 'no' or 'not sure', do you believe that a system of data altruism should be set up at national level?

☐ Yes

☐ No

☐ Not sure

39.2 If you answered 'yes' to question 39.1, how should this be managed? Please explain.

If you answered 'yes' to question 39, please provide further detail on the data altruism system in place by answering the questions below and providing details in the box.

39.3 The data altruism system has been created in my MS at:

☐ National level

☐ Regional level

☐ Sub regional level

☐ Other - please specify below

39.4 The data altruism system provides access for:

☐ All researchers

☐ Public sector researchers only

☐ Other categories – please specify below

39.5 The data altruism system provides single point of entry for researches to access data:

☐ Yes

☐ No

☐ Not sure

39.6 If yes, please explain what its functions are:

39.7 The data altruism system hosts data:

☐ Yes

☐ No

☐ Not sure

39.8 The data altruism system provides access to data that remains stored with the original data controller:

☐ Yes
☐ No
☐ Not sure

39.9 Patient who provide their access to data concerning them are offered (more than one may apply):
☐ Monetary compensation
☐ Non-monetary compensation - please specify below
☐ Other categories – please specify below
☐ Not sure

39.10 If yes, please explain

Data quality and origin

40. Has your MS adopted legislation that in any way requires that data processed for research purposes are processed in a way that ensures the FAIR principles that data are Findable, Accessible, Interoperable and Reusable?
☐ Yes
☐ No
☐ Not sure

40.1 If yes, please explain

40.2 If yes, does this legislation apply only to publicly funded research?
☐ Yes
☐ No
☐ Not sure

41. Has your MS adopted any system to facilitate the re-use of electronic health record data for research purposes?
☐ Yes
☐ No
☐ Not sure

41.1 If yes, please describe

42. Has any legislation been adopted in your MS which requires privately funded researchers to share the research data with public bodies?

- ☐ Yes
- ☐ Not obliged that may choose to do so
- ☐ No
- ☐ Not sure

42.1 If yes, please name and describe the legislation

Section F - Your opinion on future development needs

43. Do you believe that exchange health data for patient care or research **within your MS** is made difficult because of the use of different legal bases between different controllers?

- ☐ Yes
- ☐ No
- ☐ Not sure

43.1 If yes, please detail why and what should be the measures at national and EU level to overcome them

44. Do you believe that exchange health data for patient care or research **between MS** is made difficult because of the use of different legal bases between different controllers?

- ☐ Yes
- ☐ No
- ☐ Not sure

44.1 If yes, please detail why and what should be the measures at national and EU level to overcome them

45. Do you believe that exchange health data for patient care or research **between MS** is made difficult due to different governance structures in different Member States?

☐ Yes

☐ No

☐ Not sure

45.1 If yes, please detail why and what should be the measures at national and EU level to overcome them

46. Do you believe the current legislation in place in your Member State is sufficient to facilitate the free flow of health data between Member States?

☐ Yes

☐ No

☐ Not sure

46.1 If no, do you believe an EU level code of conduct could alleviate this situation ?

☐ Yes

☐ No

☐ Not sure

46.2 If yes, please describe the core issues you would want such a code of conduct to address

47. Do you believe that the current legislation in place at EU level is sufficient to facilitate the free flow of health data between Member States?

☐ Yes

☐ No

☐ Not sure

47.1 If no, do you believe that EU legislation could alleviate this situation ?

☐ Yes

☐ No

☐ Not sure

47.2 If yes, please describe the core issues you would want such a legislation to address.

Question 48-51 relate to the topics addressed in section B (planning, management, administration and improvement of the health and care systems).

48. Do you believe that the national epidemiological institutions in your MS have access to all the health data they need of citizens in your MS for **planning, management, administration and improvement of the health and care systems?**

☐ Yes

☐ No

☐ Not sure

48.1 If no, please specify what additional data you believe they should have access to and if it should be personal data, pseudonymised, anonymised or aggregated.

48.2 Do you believe any legislative change is needed at national level to address access to health data for **planning, management, administration and improvement of the health and care systems?**

☐ Yes

☐ No

☐ Not sure

48.3 If yes, what key changes would you wish to see

48.4 Do you believe any legislative change is needed at EU level to address access to health data for **planning, management, administration and improvement of the health and care systems?**

☐ Yes

☐ No

☐ Not sure

48.5 If yes, what key changes would you wish to see

49. Do you believe that the respective national institutions (medicine agencies, HTA bodies, notified bodies) in your MS have access to all the health data of citizens in your MS that they need for **market approval of medicines and devices?**

☐ Yes

☐ No

☐ Not sure

49.1 If no, please specify what additional data you believe they should have access to and if it should be personal data, pseudonymised, anonymised or aggregated.

49.2 Do you believe any legislative change is needed at national level to address access to health data for **market approval of medicines and devices?**

☐ Yes

☐ No

☐ Not sure

49.3 If yes, what key changes would you wish to see

49.4 Do you believe any legislative change is needed at EU level to address access to health data for **market approval of medicines and devices?**

☐ Yes

☐ No

☐ Not sure

49.5 If yes, what key changes would you wish to see

50. Do you believe that the national epidemiological institutions in your MS have access to all the health data of citizens in your MS that they need to **monitor medical device safety and/or pharmacovigilance?**

☐ Yes

☐ No

☐ Not sure

50.1 If yes, please specify what additional data you believe they should have access to and if it should be personal data, pseudonymised, anonymised or aggregated.

50.2 Do you believe any legislative change is needed at national level to address access to health data to **monitor medical device safety and/or pharmacovigilance**?

☐ Yes

☐ No

☐ Not sure

50.3 If yes, what key changes would you wish to see

50.4 Do you believe any legislative change is needed <u>at EU level</u> to address access to health data to **monitor medical device safety and/or pharmacovigilance**?

☐ Yes

☐ No

☐ Not sure

50.5 If yes, what key changes would you wish to see

51. Do you believe that the national epidemiological institutions in your MS have access to all the health data they need of citizens in your MS in order to respond to a health crisis (such as COVID-19)?

☐ Yes

☐ No

☐ Not sure

51.1 If no, please specify what additional data you believe they should have access to and if it should be personal data, pseudonymised, anonymised or aggregated.

51.2 Do you believe any legislative change is needed <u>at national level</u> to address access to health data for health crisis response purposes?

☐ Yes

☐ No

☐ Not sure

51.3 If yes, what key changes would you wish to see

51.4 Do you believe any legislative change is needed <u>at EU level</u> to address access to health data for health crisis response purposes?

☐ Yes

☐ No

☐ Not sure

51.5 If yes, what key changes would you wish to see

51.6 Do you believe that the data the ECDC receives currently based on the Regulation No 851/2004 and of the Decision No 1082/2013/EU is sufficient to respond to a crisis such as COVID-19?

☐ Yes

☐ No

☐ Not sure

51.7 If yes, please specify what additional access to personal data ECDC should have access to, and what key changes to the EU level legislation you would wish to see

52. Should a system of one entry points (central data hub) at national level for research data be supported in the context of the European Health Data Space?

☐ Yes, as we have one

☐ Yes, it would be desirable to have one

☐ Yes, it would be desirable, but not feasible from a political point of view

☐ No, our system is decentralised

☐ No, the researchers know their way

☐ Not sure

☐ Other, please explain

53. As noted in Section E some MS have established data governance and access bodies. Do you believe it would be useful to bring such bodies together at EU level?

☐ Yes

☐ No

☐ Not sure

53.1 If yes, do you believe an EU level data governance and access body could address the challenges that you have identified above concerning the primary and secondary use of health data?

☐ Yes, for primary use of health data

☐ Yes, for secondary use of health data

☐ Yes, for both

☐ No

☐ Not sure

54. If an EU level data governance and access body were to be set up, what form should it take at EU level?

☐ A voluntary network, for primary and secondary use of health data

☐ Two voluntary networks, for primary and secondary use of health data with some common activities

- ☐ A form of public-private partnership
- ☐ An EU committee
- ☐ An EU agency
- ☐ Other, please explain

55. Please explain what should be the functions of an EU level cooperation (multiple replies are possible)?
    - ☐ To exchange best practices
    - ☐ To support in implementing data protection rules for access to health data across borders
    - ☐ To elaborate interoperability agreements
    - ☐ To elaborate agreements for data access
    - ☐ To elaborate minimum datasets for data exchange
    - ☐ To support policy makers and regulators to access data
    - ☐ Other, please explain

56. The EU's single Digital Gateway Regulation (EU 2018/1724) promotes a principle of entering data 'once only'[35] and promoting re-use of data where possible. Do you see any relevance of the EU's single Digital Gateway Regulation (EU 2018/1724) for the exchange of health data between healthcare providers within or between Member States?
    - ☐ Yes
    - ☐ No
    - ☐ Not sure

    56.1 If yes, please explain

57. Section E also addressed data altruism. Do you believe that a system of data altruism should be set up at EU level?
    - ☐ Yes
    - ☐ No
    - ☐ Not sure

[35] The once-only principle is among the seven underlying principles of this action plan to make government more effective, simpler and reduce administrative burdens for citizens and businesses by re-using data within government. The principle requires public administrations to "ensure that citizens and businesses supply the same information only once […]. Public administration offices take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses"

57.1 If yes, how should this be managed, please explain

Survey Part TWO

A practical and technical analysis of how the processing of health data is governed at national level.

Background to Part TWO - practical and technical issues

In this part of the survey we would like to explore the level of practical and technical readiness to share health related data, looking at how the processing of health data is governed at national level. We are keen to map the way in which health data is governed in a practical manner at the national level such as mechanisms to assure health data interoperability and health data sharing.

*Please note the definition of terms shown on page 1, including **Healthcare provider** used to mean any natural or legal person or any other entity legally providing and **Healthcare professional** used to mean a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife, or a pharmacist or other person considered to be a health professional according to the legislation of your MS*

This part of the survey is divided into 4 sections which deal with the following issues:

A. Use of Electronic Health Records(EHRs) and other digital health tools
B. Standards for interoperability, security and quality of EHRs and health data
C. Research based on health data in EHRs and other data repositories – by both public and private entities
D. General questions and your opinions

Section A: Electronic Health Records

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The questions in this section seek to get a picture of the extent to which EHRs are used in your MS and for which purposes. We also wish to learn about the use of Personal Health Records or other patient accessible tools, as well as other core digital health tools (ePrescriptions, disease registries etc). The questions concern EHRs used for the primary purpose of care provision, as well as EHRs used for the secondary purposes which are examined in sections B and C.

58. In your MS are there ICT systems by which healthcare professionals can share the electronic Health Records (EHR) of individual patients with other healthcare professionals?

☐ There is **one national** system to share EHRs between healthcare professionals across different healthcare providers (primary, secondary or tertiary care and long-term care). *Please name and describe that system in the box below.*

☐ There are **several national** systems to share EHRs between healthcare professionals across healthcare providers (primary, secondary or tertiary care and long-term care*). Please name and describe those systems in the box below.*

- ☐ There are **several sector specific national** systems to share EHRs between healthcare professionals in specific healthcare provider sectors (primary, secondary or tertiary care and long-term care providers). *Please name and describe those system in the box below.*
- ☐ There are **several sector specific regional systems** to share EHRs between healthcare professionals in specific healthcare provider sectors (primary, secondary or tertiary care and long-term care providers). *Please name and description those systems in the box below.*
- ☐ There are several systems, administered by **separate ICT vendors or service providers.** Please name and description those systems in the box below.
- ☐ EHRs are not routinely used.
- ☐ EHRs are used, but no systems are in place to allow for sharing EHRs between healthcare providers.
- ☐ None of the above.
- ☐ I don't know.

Further details:

59. Please evaluate on the scale below the extent to which you believe EHRs are routinely shared between healthcare professionals in your MS when patients move between healthcare professionals **within the same healthcare provider or provider group**.
    - ☐ EHRs are shared for all care transfers between healthcare professionals.
    - ☐ EHRs are shared for **more than 75% transfers** between healthcare professionals.
    - ☐ EHRs are shared for **less than 25%** care transfers between healthcare professionals.
    - ☐ EHRs are shared for **less than 10% care transfers** between healthcare professionals.
    - ☐ I don't know.

Additional comments on this subject:

60. Please evaluate on the scale below the extent to which you believe EHRs are routinely shared between healthcare professionals in your MS when patients move between healthcare professionals when moving to a **different healthcare provider or provider group.**
    - ☐ EHRs are shared for all care transfers between healthcare professionals.
    - ☐ EHRs are shared for **more than 75% transfers** between healthcare professionals.
    - ☐ EHRs are shared for **less than 25%** care transfers between healthcare professionals.
    - ☐ EHRs are shared for **less than 10% care transfers** between healthcare professionals.
    - ☐ I don't know.

Additional comments on this subject:

61. Please name and describe any institution which exists in your MS to oversee the exchange of data for the provision of healthcare:

62. Do you believe that such institutions should cooperate at EU level and if so, what would be the form and structure of such a cooperation?

63. In your MS, is there an ICT system through which **patients can access their EHR** data?

- ☐ Yes, this is organised nationally. Please name and describe those systems in the box below
- ☐ Yes, this is organised regionally. Please name and describe those systems in the box below
- ☐ Yes, this is organised by individual health services. Please name and describe those systems in the box below
- ☐ No, there are no such ICT systems
- ☐ Other - please specify in the box below
- ☐ I don't know.

Further details/comments:

64. If you answered yes above, do patients have access to the full EHR or just specific parts?

- ☐ Full EHR
- ☐ Partial EHR
- ☐ I don't know.

65. Please evaluate on the scale below the extent to which you believe **EHRs or partial EHRs are accessed by patients** in your MS?

- ☐ Many patients access their EHRs on a regular basis.
- ☐ Some patients access their EHR on a regular basis.
- ☐ (very) few access their EHR on a regular basis

Further details/comments:

66. Can **patients add information** or comments to the EHR by themselves?

- ☐ Yes
- ☐ No
- ☐ Not sure

Further details/comments:

67. Citizens increasingly use apps and devices to track and record issues like food intake, exercise, sleep etc. Please indicate how such data may be included into EHRs. (multiple answers may apply).

- ☐ Healthcare professionals are **obliged** to incorporate patient generated data into healthcare professional/ provider held EHRs.
- ☐ Healthcare professionals are **allowed** to incorporate patient generated data into healthcare professional/ provider held EHRs.
- ☐ Healthcare providers **can – in a technical sense –** incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so
- ☐ It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs.
- ☐ I don't know.

Additional comments on this subject:

68. Does your country participate or plan to participate in European infrastructures such as an eHDSI (eHealth Digital Service Infrastructure), also known as MyHealth@EU?

- ☐ Yes, for sharing summary records
- ☐ Yes, for sharing prescriptions
- ☐ Yes, for other reasons, please specify below
- ☐ No
- ☐ Not sure

Additional comments on this subject:

69. Please evaluate on a scale of 1-10 the ease with which you believe a healthcare professional in your MS could share data from an EHR with a healthcare professional in another MS for patient care. 1 = very easily 10 = impossible

Scale 1-10: _____

Additional comments on this subject:

Section B : Technical standards

A number of general and sectoral Standards Development Organisations, such as ISO, CEN, HL7 and CDICS, have developed technical standards to drive interoperability, security and quality of health records and other health data exchange infrastructures. Many countries have adopted policies, guidelines or legal requirements that ensure such standards are used by healthcare provider organisations. The questions in this section look the adoption of such policies to ensure use of technical standards to support interoperability of health data, as well as security and quality.

70. Are there national or regional **interoperability policies** regarding the technical standards to be used to ensure that the structure and format of data are interoperable so that such data may be **shared** between healthcare professionals or incorporated into more than one database for secondary use?

- ☐ There is **one national data interoperability policy** which addresses use of standards and interoperability across **all healthcare provider sectors** (primary, secondary, tertiary, long term care) (please specify below)
- ☐ There are **several national data interoperability policies** which address use of standards and interoperability for **each healthcare provider sector** (primary, secondary, tertiary, long term care) healthcare sectors.
- ☐ Each **region has one data interoperability policy** which addresses use of standards and interoperability across **all healthcare provider sectors** (primary, secondary, tertiary, long term care) (please specify below
- ☐ Each **region has several data interoperability policies** which address use of standards and interoperability for **each healthcare provider sectors** (primary, secondary, tertiary, long term care) healthcare sectors.
- ☐ No, there are no national or regional policies to ensure use of standards for data interoperability
- ☐ I don't know

Please specify which technical standards for interoperability are addressed in policies in your MS *If none of the above apply, please describe any other actions adopted to promote interoperability of health data*

71. Are there national or regional **health data security policies** regarding the **technical standards** to be used to ensure health data for primary use are processed and stored securely.

- ☐ There is **one national data security policy** which addresses use of security standards across **all healthcare provider sectors** (primary, secondary, tertiary, long term care) (please specify below).
- ☐ There are **several national data security policies** which address use of security standards in **each healthcare provider sector** (primary, secondary, tertiary, long term care) healthcare sectors.
- ☐ Each **region has one data security policy** which addresses use of security standards across **all healthcare provider sectors** (primary, secondary, tertiary, long term care) (please specify below.

- ☐ Each **region has several data security policies** which address use of security standards in **each healthcare provider sectors** (primary, secondary, tertiary, long term care) healthcare sectors.
- ☐ No, there are no national or regional data security policies to ensure use of standards for data security.
- ☐ I don't know.

Please specify which technical standards for data security are addressed in policies in your MS *If none of the above apply, please describe any other actions adopted to promote security of health data*

72. Are there national or regional **data quality policies** regarding the technical standards to be used to ensure the quality of health data for use in EHRs or other digital applications
    - ☐ There is **one national data quality policy** which addresses use of standards across **all healthcare provider sectors** (primary, secondary, tertiary, long term care) (please specify below).
    - ☐ There are **several national data quality policies** which address use of standards for **each healthcare provider sector** (primary, secondary, tertiary, long term care) healthcare sectors.
    - ☐ Each **region has one data quality policy** which addresses use of standards across **all healthcare provider sectors** (primary, secondary, tertiary, long term care) (please specify below.
    - ☐ Each **region has several data quality policies** which address use of standards for **each healthcare provider sectors** (primary, secondary, tertiary, long term care) healthcare sectors.
    - ☐ No, there are no national or regional policies to ensure use of quality standards for health data.
    - ☐ I don't know

Please specify which technical standards for data quality are addressed in policies in your MS *If none of the above apply, please describe any other actions adopted to promote quality of health data*

73. If you have answered 'yes' to any of the questions in this section above, please name and describe the agency or agencies which oversees the implementation of such standards policies.

Section C: Data access infrastructure for secondary use of data

Health data collected for care provision can often be re-used for research, this is generally referred to as a secondary use. Such secondary use may be exercised by public entities such as national health systems statutory payers (public bodies of health insurers), public research entities (including universities, public health laboratories), by regulators such as medicines agencies and notified bodies as well as by industry. The term industry includes large and small pharmaceutical and medical technology companies, companies in the insurance and financial services sector, as well as the social media and consumer electronics actors, and the emerging AI industry. In many countries a centralised data access infrastructure has been established to facilitate access to such data. Below we ask about such infrastructure in your MS and its use by public sector entities for healthcare planning, management, monitoring or improvement purposes; by regulatory bodies such as medicines agencies and notified bodies for monitoring quality and effectiveness of medicines and medical devices; or by public and private sectors researchers (academic and commercial) for scientific research purposes

74. In your MS are entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)?

- ☐ There is **one national** system to share data for secondary use *Please name and describe that system in the box below.*
- ☐ There are **several national** systems to share data for secondary use. *Please name and describe those systems in the box below.*
- ☐ There are **several sector specific national** systems to share data for secondary use. *Please name and describe those system in the box below.*
- ☐ There are **several sector specific regional systems** to share data for secondary use.
- ☐ There are several systems for sharing data for secondary use, administered by **separate ICT vendors or service providers.** Please name and description those systems in the box below.
- ☐ None of the above (please describe the situation below).
- ☐ I don't know

75. In your MS, is there a centralised data access infrastructure through which data can be accessed for secondary use purposes.

- ☐ Yes (please go to question 76 to 86)
- ☐ No (please go to question 87 to 93)

Questions 76-86 for MS that have a centralised data access infrastructure

76. Please indicate **all the data sources** which can be accessed via the centralised data access infrastructure

- ☐ Primary care electronic health records
- ☐ Hospital electronic health records
- ☐ Social or long-term care
- ☐ Health insurance claims data
- ☐ Prescribing and dispensation records
- ☐ Disease registries
- ☐ Bio banks
- ☐ Disease registries
- ☐ Genomic data bases
- ☐ Linked health, social and environmental data
- ☐ Other, please specify below

Additional comments on this subject:

77. Please indicate who may access the centralised data access infrastructure

- ☐ Accessible by all types of organisations
- ☐ For public sector organisations only

Additional comments on this question:

78. Please indicate the types of research that may be conducted using the centralised data access infrastructure (more than one answer may apply)

- ☐ Research for health system monitoring, management and evaluation by a public sector entity
- ☐ Research for medicines and device monitoring and evaluation (including pharmacovigilance) by public sector organisations (including regulators)
- ☐ Scientific research by not-for -profit academic organisations
- ☐ Commercial scientific organisations (including pharmaceutical and medical technology industry)
- ☐ Any commercial enterprise

Additional comments on this question:

79. Please indicate what type of organisation what type of runs the centralised data access infrastructure

- ☐ Government directly
- ☐ A governmental agency
- ☐ A private sector entity
- ☐ A public-private-partnership

☐ Other – please describe below

Additional comments on this subject:

80. How are the rules of governance for the centralised data access infrastructure created?
- ☐ Provided by the legislation which set up the centralised data access infrastructure
- ☐ Set by the private actors which set up centralised data access infrastructure
- ☐ Set by the original data controllers
- ☐ Other, please specify below

Additional comments on this subject:

81. Who bears the costs for the infrastructure? (more than one option is possible)
- ☐ Government
- ☐ The private actors which have set it up
- ☐ Private actors but subsidized by government
- ☐ Fees paid by the parties accessing the data
- ☐ I don't know

Additional comments on this subject:

82. Where fees are payable by the parties who access the data, the fees are:
- ☐ The same for all data users
- ☐ Differentiated, depending on the entity requesting the data - e.g. public authority, public researcher, private researcher, industry etc. (please describe further below)
- ☐ No fee is payable

Additional comments on this subject:

83. What does the fee cover?
- ☐ Cost of searching
- ☐ Cost of curating health data
- ☐ Cost of infrastructure
- ☐ Other, please describe below

84. Please indicate with which, if any, label the data held in the centralised data access infrastructure are marked:
- ☐ Patient's full name
- ☐ Patient's national civic number or patient ID

- ☐ An algorithmic pseudonym of the patient's name
- ☐ An algorithmic pseudonym of the patient's ID number
- ☐ A pseudonym created from several factors
- ☐ Fully anonymised

Additional comments on this subject:

85. If a pseudonym is used, can it be used to link data across various data sources?
    - ☐ Yes
    - ☐ No

Additional comments on this subject:

86. If private actors (industry) would want to use the infrastructure for pharmacovigilance, medical device and medicines safety:
    - ☐ That would be possible under the same conditions as for public entities
    - ☐ That would be possible under different conditions, please specify as much as possible below

Additional comments on this subject:

☐ **Questions 87-93 for MS where there is no centralised data access infrastructure**

87. Please indicate the process used to access **data held in EHRs** for secondary use (more than one answer may apply)
    - ☐ Application to the data controller - healthcare provider or healthcare professional
    - ☐ Application to a research ethics body
    - ☐ Application to the national Data Protection Authority
    - ☐ Other - please describe in the box below

Additional comments on this question:

88. Please indicate who may apply for access **data held in EHRs** for secondary research purposes
    - ☐ Accessible by all types of organisations
    - ☐ For public sector organisations only
    - ☐ Other classification – please describe below

Additional comments on this question:

89. Please indicate the types of research that may be conducted using data held in **EHRs** (more than one answer may apply)

- ☐ Research for health system monitoring, management and evaluation by a public sector entity
- ☐ Research for medicines and device monitoring and evaluation (including pharmacovigilance) by public sector organisations (including regulators)
- ☐ Scientific research by not-for -profit academic organisations
- ☐ Commercial scientific organisations (including pharmaceutical and medical technology industry)
- ☐ Any commercial enterprise
- ☐ Other

Additional comments on this question:

90. Please indicate the process used to access health data held in **disease registries** for secondary research purposes (more than one may apply)

- ☐ Application to the data controller of the disease registry
- ☐ Application to a research ethics body
- ☐ Application to the national Data Protection Authority
- ☐ Other - please describe in the box below

Additional comments on this question:

91. Please indicate who may apply for access data held in **disease registries** for secondary research purposes.

- ☐ Accessible by all types of organisations
- ☐ For public sector organisations only
- ☐ Other classification – please describe below

Additional comments on this question:

92. Please indicate the types of research that may be conducted using data held in **disease registries** (more than one answer may apply).

- ☐ Research for health system monitoring, management and evaluation by a public sector entity
- ☐ Research for medicines and device monitoring and evaluation (including pharmacovigilance) by public sector organisations (including regulators)
- ☐ Scientific research by not-for -profit academic organisations
- ☐ Commercial scientific organisations (including pharmaceutical and medical technology industry)
- ☐ Any commercial enterprise

Additional comments on this question:

93. Please explain how access to health data in EHRs or Disease Registries or any other data repository **for monitoring of medical device safety and/or pharmacovigilance** is ensured in your MS.

Section D: Opinions

In this final section we would like to gather your personal opinions on some core issues to do with the way in which health data sharing is organised in your MS and on the statements below. The objective is to gain a snapshot of key pain points, rather than scientifically valid assessment.

94. To what extent do you agree with the following statements (5-point scale. 1 completely disagree; 5 completely agree).

Statement:	1= strongly disagree; 5= strongly agree
It is easy to gain access to health data for research and statistics in the public domain.	
It is easy to gain access to health data for research by not-for-profit or academic entities.	
It is easy to gain access to health data for research by commercial entities	
The regulatory and organisational landscape for using health data for research is fragmented.	
GDPR is a significant obstacle for the use of health data for research and statistics in the public domain.	
Lack of interoperability between health data is a significant obstacle in my country	
Healthcare organisations are reluctant to share data for research purposes	
The time and interaction costs of gaining access to health data for research are high.	
The financial costs of gaining access to health data for research are high.	

95. What action on the EU level would be helpful to improve and stimulate the use of health data for research and statistics in the public domain in your country (e.g. guidelines, recommendations, legislation, a Code of Conduct)? Please describe below:

96. Please name (if possible, with URL) one or two organisations or registries that can be considered exemplary for your country with respect to **secondary use of**:

- ☐ Primary care data. URL…
- ☐ Hospital and medical specialist care. URL….
- ☐ Prescription drugs. URL…
- ☐ Self-measurements. URL…

Additional comments on this subject:

Thank you for responding to this survey.

If you have any overarching comments or reflections, we'd appreciate if you could fill them in below

ANNEX 4 EXPERT AND STAKEHOLDER SURVEY

Stakeholder Survey EUHealthSupport

Fields marked with * are mandatory.

Survey assessing the Member States' rules on health data in the light of GDPR

The European Commission has initiated a study that aims to examine in which manners the processing of personal health date is governed across the EU and how this might affect the cross-border exchange of health data in the EU.

The present survey is targeted at experts and organisations representing the wide range of stakeholders, including patients, care providers and researchers. Objective of the survey is to identify gaps and needs concerning the use of health data within the EU, the manner in which citizens have control over their health data and to explore strategies and governance structures for the use and re-use of health data.

The survey, among others, seeks your opinion in what areas EU level action might be needed in order to govern the processing of health data across the EU. It also contains a series of statements on data sharing for different types of use, as described below:

- Data processing for the purposes of **provision of health and social care** by health and care providers to the patient concerned. This includes both in-person care and telecare using eHealth or mHealth tools.
- Data processing for **wider public health purposes** including planning, management, administration and improvement of health and care systems; prevention or control of communicable diseases; protection against serious threats to health and ensuring high standards of quality and safety of healthcare and of medical products and medical devices.
- Data processing for **scientific or historical research** by both public and private sector organisations (third parties, not being the original data controller), including the pharmaceutical and medical technology industries and insurance providers.

Results of the study will be used in a report to be submitted to the European Commission in the summer of 2020.

Note. As some questions may require more information about existing legislation or procedures, it is possible to skip any questions you wish, or to respond 'don't know.

Thank you for your contributions to this study

On behalf of the EUHealthSupport team,

Johan Hansen, Robert Verheij (Nivel, Netherlands institute for health services research), Petra Wilson (Health Connect Partners), Evert-Ben van Veen (MLC Foundation) Contact: contact@euhealthsupport.eu

SECTION A: QUESTIONS ABOUT YOUR BACKGROUND WHEN PROVIDING ANSWERS

The following questions are mandatory to be able to interpret the results of the survey. To guarantee your anonymity we will only report on each of these questions separately. Hence, while we may report how respondents from public bodies perceive the issues or respondents from specific countries, the combination of both will in no way be revealed.

* 1. Please indicate the membership your organisation represents, if any (tap on the box below to choose your answer):

- ○ No organisation, I am answering as individual citizen
- ○ Patient organisation
- ○ Health professional
- ○ Healthcare providers
- ○ Healthcare insurers
- ○ Scientific researchers
- ○ Industry
- ○ Public Administration/Governmental organisation/MoH
- ○ Other, please specify

Patient organisation category

- ☐ Disease specific
- ☐ General

Health professionals category:

- ☐ Nurses
- ☐ Generalist doctors
- ☐ Specialist doctors
- ☐ All
- ☐ Other

Healthcare providers category

- ☐ Public
- ☐ Private
- ☐ All
- ☐ Other

Healthcare insurers category:

- ☐ Public
- ☐ Private
- ☐ All
- ☐ Other

Scientific researchers category

- ☐ Public
- ☐ Private
- ☐ All
- ☐ Other

Industry category:

- [ ] Pharmaceutical
- [ ] Biotech
- [ ] Med Tech
- [ ] Other

Public administration category:

- [ ] Ministry
- [ ] E-health agency
- [ ] One entry point for secondary use of data
- [ ] Medicine agency
- [ ] Notified body
- [ ] Epidemiological institution
- [ ] Other

Other, please specify..

* 2. Please indicate the geographical level you or your organisation represents

- ( ) An EU Member State (or part of an EU Member State)
- ( ) A non-EU country
- ( ) EU / Multiple European countries
- ( ) International

* 3. I live in the following country:

- ( ) Austria
- ( ) Belgium
- ( ) Bulgaria
- ( ) Croatia
- ( ) Cyprus
- ( ) Czechia
- ( ) Denmark
- ( ) Estonia
- ( ) Finland
- ( ) France
- ( ) Germany
- ( ) Greece
- ( ) Hungary
- ( ) Ireland
- ( ) Italy
- ( ) Latvia
- ( ) Lithuania
- ( ) Luxembourg
- ( ) Malta
- ( ) Netherlands
- ( ) Norway
- ( ) Poland
- ( ) Portugal
- ( ) Romania
- ( ) Slovak Republic
- ( ) Slovenia
- ( ) Spain
- ( ) Sweden
- ( ) Switzerland

- United Kingdom
- Other

If other, please specify

SECTION B: SHARING HEALTH RELATED DATA FOR THE PURPOSE OF PROVIDING CARE

In order to provide healthcare to patients, healthcare professional require access to data collected by other healthcare professionals both within their country and in other countries where the patient might have received or want to receive care. This is referred to as data processing for the **primary purpose for which** data were collected.

4. Do you agree or disagree with the following statements, all related to the way in which such data sharing for providing care is possible and how it could be improved? *Note: If the statement concerns 'my country' and you are answering at an EU or international level, please answer for the country in which you currently live. It is also possible to skip a question.*

Data portability allows data subjects to receive personal data they provided to a controller in a structured, commonly used and machine-readable format and to transmit those data to another controller.

Interoperability refers to the ability of different information systems, devices and applications to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organisational, regional and national boundaries.

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
It is easy for a patient to access his or her medical record **in my country**						
It is easy for a patient **in my country** to obtain a portable copy of their medical record to take to another healthcare provider in the same country						
It is easy for a patient to obtain a portable copy of their medical record to take to another healthcare provider in **a different EU country**						
The medical records in my country are structured around the patient (e.g as personal data space or patient portal)						

Having health data in a personal data space /patient portal facilitates the transfers between healthcare providers	○	○	○	○	○	○
Lack of data portability **drives up costs** through repeat testing and examination	○	○	○	○	○	○
Lack of data portability **slows down time** to diagnosis and treatment	○	○	○	○	○	○
Lack of data portability **increases the risk of errors**	○	○	○	○	○	○
Lack of data portability can **limit the rights** of Europeans to seek care in another EU country	○	○	○	○	○	○
Lack to data portability can **limit the rights** to Europeans to work or go on holiday in another EU country	○	○	○	○	○	○
Sharing of data for care provision purposes **within my country** is very difficult because of low levels of interoperability between health record systems	○	○	○	○	○	○
Sharing of data for care provision purposes **with another EU country** is very difficult because of low levels of interoperability between health record systems	○	○	○	○	○	○
Sharing of data for care provision purposes **within my country** is a major privacy risk because of insufficient security measures (including cloud security)	○	○	○	○	○	○

Sharing of data for care provision purposes **with another EU country** is a major privacy risk because of insufficient security measures (including cloud security)	○	○	○	○	○	○
The use of different legal bases (e.g. consent, provision of care, public interest) make it difficult for health-related data to be **shared for care purposes** between EU countries	○	○	○	○	○	○
Additional measures should be taken at **national level** to enforce patients' access and control over their own health data and portability of this data	○	○	○	○	○	○
Additional measures should be taken at **EU level** to enforce patients' access and control over their own health data and portability of this data	○	○	○	○	○	○

5. Would you like to provide further details on data sharing for providing care and control of patients over their own data? E.g., what types of actions are needed to improve, with particular focus on health data sharing at EU level?

SECTION C: DATA PROCESSING FOR SCIENTIFIC OR HISTORICAL RESEARCH

Health data collected for the primary purpose of providing care are sometimes used for the **secondary purpose of scientific (or historical) research**. This includes research undertaken by public or private sector organisations, including the pharmaceutical and medical technology industries and insurance providers.

6. Do you agree or disagree with the following statements, all related to the way in which such data sharing for scientific research is possible and how it could be improved? *Note: If the statement concerns 'my country' and you are answering at an EU or international level, please answer for the country in which you currently live. It is also possible to skip a question.*

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
It is easy to gain access to health data for researchers working in the **public domain** in my country						
It is easy to gain access to health data for research for researchers working **in not-for-profit or academic entities** in my country						
It is easy to gain access to health data for research by **commercial entities** in my country						
It is easy to gain access to health data for research by **industry (pharma, medical devices, Artificial Intelligence)** inmy country						
The current data protection rules in my country make **data access for research** purposes difficult						
The current data protection rules in my country **do not adequately protect** the interest of patients						
The **time and interaction costs** of gaining access to health data for research are high in my country						
The **financial costs** of gaining access to health data for research are high in my country						
Different rules for access to data for research purposes for **public sector and private sector researchers** should apply in my country						

There is a need for an **EU level** regulatory and organisational landscape for using health data for research						
A system to allow patients to make data available for research without reference to a particular research project (also known as data altruism) **shouldexist in my country**						
A system to allow patients to make data available for research without reference to a particular research project (also known as data altruism) **should exist at EU level**						
Rules **in my country** make access to data for research organisations unnecessary complex						
EU rules make access to data for research organisations unnecessary complex						
The current **national rules** are outdated, given new developments such as personalised medicine, Artificial Intelligence etc.						
The current **EU rules** are outdated, given new developments such as personalised medicine, Artificial Intelligence etc.						
A single point of contact for the use of health data for research should be supported **in my country**						

Single points of contact should be set up in **all Member States**, making access to health data for research much simpler	○	○	○	○	○	○
All single points of contact should be **linked at EU level**, to support pan- European research	○	○	○	○	○	○
One single point of contact should also be set up **at EU level**, in addition to national ones	○	○	○	○	○	○

7. Would you like to provide further details on data sharing and control of patients over their own data for scientific research? E.g., what types of actions are needed to improve, with particular focus on health data sharing at EU level?

SECTION D: SHARING DATA FOR THE PUBLIC HEALTH PURPOSES OF ENSURING A SAFE HEALTHCARE SYSTEM

Health data originally collected for the primary purpose of providing care are sometimes used for wider public health purposes, being:

1. Supporting health care system planning, the planning, management, administration and improvement of health and care systems.
2. Ensuring high standards of quality and safety of healthcare and of medical products and medical devices.
3. The prevention or control of communicable diseases and the protection against serious (cross- border) health threats.

Questions below address all of these three functions.

8. Do you agree or disagree with the following statements, all related to the way in which data sharing is possible for the above mentioned wider public health purposes? Note. If the statement concerns 'my country' and you are answering at an EU or international level, please answer for the country in which you currently live.

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
It is easy **for the concerned professionals** to gain access to health data for public health planning, quality and prevention purposes in my country	○	○	○	○	○	○
Data access **for public health purposes** is difficult because data sets are scattered over many different providers in my country	○	○	○	○	○	○
Use of data for **national level** public health purposes is difficult because data are not comparable between different data sets	○	○	○	○	○	○
Use of data for **cross-border** public health purposes is difficult because data are not comparable between different data sets	○	○	○	○	○	○
The use of **different legal bases** (eg consent, provision of care, public interest) makes it difficult for health-related data to be shared for public health purposes between EU countries	○	○	○	○	○	○

Different **interpretations of whether data are considered anonymised or pseudonymised** make it difficult for health-related data to be shared for public health purposes between EU countries	○	○	○	○	○	○
Epidemiological institutions should have easier and direct access to health data, in order to ensure their task	○	○	○	○	○	○
Medicine agencies, notified bodies for medical devices or Health Technology Assessment bodies should have easier and direct access to health data, in order to ensure their task	○	○	○	○	○	○
Governance structures, data permit authorities, or single points of contact should ensure that **public bodies** are allowed to have easier and direct access to health data	○	○	○	○	○	○

9. Would you like to provide further details on data sharing for one or more of the following types of public health purposes?

9.a. The purpose of supporting health care system planning, the planning, management, administration and improvement of health and care systems.

9.b.The purpose of ensuring high standards of quality and safety of healthcare and of medical products and medical devices.

9.c. The purpose of prevention or control of communicable diseases and the protection against serious (cross-border) health threats.

SECTION E – POTENTIAL EU LEVEL ACTION

At present, EU level legislation on data use for function 2 or 3 (secondary use) is governed by a combination of the GDPR and national level legislation foreseen in the GDPR to address issues such as the use of data for the purposes of healthcare provision (provided for in Article 9(2)(h)) or in the public interest (provided for in Article 9(2)(i)) or for scientific research (provided for in Article 9(2)(j)). The European Commission's Data Strategy envisions a European Health Data Space which may demand a range of actions at EU level.

10. The statements below represent some of the potential actions that may be taken for the use of health data for healthcare, but also for policy making and research. Please indicate the extent to which you agree or disagree with the potential actions.

EU level action should be taken to..

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
Increase awareness of citizens rights on **data access** to their medical health records/health data under GDPR	○	○	○	○	○	○
Increase awareness of citizens' rights on **data portability** under GDPR (being able to transfer one's personal data to another controller)	○	○	○	○	○	○
Support Member States to reinforce **citizens' access, portability and control** over their health data, for example by guidance or legislation	○	○	○	○	○	○

Support Member States' healthcare providers to ensure the transfer of health data **between different healthcare providers** and at the request of patients, this to allow patients to provide their health data only once, for example by guidance or legislation	○	○	○	○	○	○
Support Member States to set up **personal data spaces** or patients' portals centred around patients, for example by guidance or legislation	○	○	○	○	○	○
Support Member State to put in place structures **allowing for secondary use** of health data for policy making and research, for example by guidance or legislation	○	○	○	○	○	○
Support Member States to set up **governance structures** for managing data available for research without a reference to a particular research project (data altruism), for example by guidance or legislation	○	○	○	○	○	○
Set up **governance structures at EU level** for managing data available for research without a reference to a particular research project (data altruism)	○	○	○	○	○	○

Support the processing of health data by **epidemiological institutions** for the protection against serious cross-border health threats, for example by guidance or legislation	○	○	○	○	○	○
Support the processing of health data by **medicine agencies, notified bodies for medical devices or Health Technology Assessment bodies** for ensuring high standards of quality and safety of health care and of medicinal products or medical devices, for example by guidance or legislation	○	○	○	○	○	○
Support the processing of health data for **scientific or historical research or statistical purposes**, for example by guidance or legislation	○	○	○	○	○	○
Support the processing of health data by **industry (pharmaceutical, medical devices, Artificial Intelligence)** to health data, for example by guidance or legislation	○	○	○	○	○	○
Set up **governance structures** to support such processing of health data by industry (pharmaceutical, medical devices, Artificial Intelligence)	○	○	○	○	○	○
Promote the use of the **same legal base** of sharing health data for research purposes	○	○	○	○	○	○

Provide EU level guidance on **obtaining consent** from patients for sharing data	○	○	○	○	○	○
Provide EU level guidance on **anonymising /pseudonymising** health data	○	○	○	○	○	○
Support **interoperability** through the use of open exchange formats / interoperability agreements, for example by guidance or legislation	○	○	○	○	○	○
Promote **data quality and reliability** through the use of standards	○	○	○	○	○	○
Promote **data security** through the use of standards health-related cybersecurity standards	○	○	○	○	○	○
Develop **minimum datasets** for data exchange	○	○	○	○	○	○

10a. If you would like to propose any other action to be taken at EU level, you can specify this below:

11. How do you think the EU should organise health data sharing for secondary purposes at EU level? *Multiple answers are possible.*

- ☐ Non-legislative policy guidance documents
- ☐ A set of common rules, put together in a Code of Conduct (soft law)
- ☐ New health data specific European level law
- ☐ A structure linking all existing health data of different countries to each other
- ☐ Setting up structures at national level intermediating access to health data (one entry point/data permit authority)
- ☐ A network of Member States representatives, structured along two pillars: use of health data for research and policy making, alongside another pillar aimed at use of data for healthcare
- ☐ A structure intermediating access to health data e.g. a body where a request for access to existing health data can be put forward and managed
- ☐ A structure managing data available for research without a reference to a particular research project (data altruism)
- ☐ An EU agency for e-health and health data
- ☐ A structure managing the health data based on consent of the patients
- ☐ Set up a network of data permit authorities/one entry points at EU level
- ☐ None of these options, the current set of rules and regulations is sufficient
- ☐ None of these options, I don't see the value of a common model for health data sharing
- ☐ Other, please specify

Other, please specify:

12. Who do you think should be involved in setting up regulations for the secondary use of data at European level? *Multiple answers are possible.*

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
Patients/patient representatives	○	○	○	○	○	○
Researchers in the area of public health	○	○	○	○	○	○
National statistics offices	○	○	○	○	○	○
International statistics offices (such as Eurostat, WHO, OECD)	○	○	○	○	○	○
(Representatives of) healthcare professionals	○	○	○	○	○	○

Regulators (medicine agencies, Health Technology Assessment and notified bodies, etc.)	○	○	○	○	○	○
Data protection authorities	○	○	○	○	○	○
National policy makers	○	○	○	○	○	○
EU policy makers	○	○	○	○	○	○
Public bodies ensuring the prevention of diseases (such as centres for disease control, national health institutes, institutes monitoring infectious diseases)	○	○	○	○	○	○
Biobanks	○	○	○	○	○	○
Commercial parties, such as pharmaceutical industry, manufacturers of wearables, tech industry, insurers	○	○	○	○	○	○

12a. If other than the above, please specify:

13. If an EU level data sharing infrastructure for secondary purposes were set up, what functions should it have?

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
A structure linking all existing health data of different countries to each other	○	○	○	○	○	○
A structure linking the one entry points/data permit authorities of different countries, other research infrastructures and data sources and EU institutions /agencies	○	○	○	○	○	○

A structure intermediating access to health data e.g. a body where a request for access to existing health data can be put forward and managed	○	○	○	○	○	○
A structure managing the health data based on consent of the patients	○	○	○	○	○	○
None of these options, the current set of rules and regulations is sufficient	○	○	○	○	○	○
None of these options, I don't see the value of a common model for health data sharing	○	○	○	○	○	○

14. If an EU level data sharing infrastructure were set up, how should it be organised? *Multiple answers are possible.*

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
A voluntary network, for both primary and secondary use of health data	○	○	○	○	○	○
Two voluntary networks, one for primary use and one for secondary use of health data with some common activities	○	○	○	○	○	○
A form of public-private partnership	○	○	○	○	○	○
An EU committee	○	○	○	○	○	○
An EU agency	○	○	○	○	○	○
None of these options, because in my view this should not be set up at EU level	○	○	○	○	○	○

14a. If other than the above, please specify:

15. If an EU level data sharing infrastructure were set up, how should its governance/rules be assured?
Multiple answers are possible.

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
A code of conduct put together by representatives of all relevant national authorities	○	○	○	○	○	○
A code of conduct put together by a board of stakeholders	○	○	○	○	○	○
EU level legislation	○	○	○	○	○	○
Other	○	○	○	○	○	○

15a. If other than the above, please specify:

16. The COVID-19 pandemic has demonstrated that access to data for responding to communicable disease outbreaks is very important. To be able to respond better to such situations in the future the EU should take action to:

	Completely disagree	Slightly disagree	Neutral	Slightly agree	Completely agree	Don't know
Ensure that pseudonymised health data on affected citizens can be shared with public health authorities without consent on the basis of public health need for public health purposes	○	○	○	○	○	○
Ensure that only non-identifiable health data on affected citizens can be shared for relevant public health purposes with public health authorities	○	○	○	○	○	○

Facilitate reporting of pseudonymised data of national and regional public health laboratories directly to ECDC without going through a reporting cascade						
Facilitate direct reporting of national and regional public health authorities to public health institutions dealing with epidemiological aspects, without going through a reporting cascade						
Set up a system at EU level to allow patients to make data available for research without reference to a particular research project (also known as data altruism)						
Set up an EU level governance managing the data altruism						
Such a data altruism system should also be used for pandemics						

Thank you for completing our questionnaire.

If you would like to receive information about the results of the study, we kindly ask you to send a message to contact@euhealthsupport.eu

In case of any comments or suggestions, we would be grateful if you could fill them in here

ANNEX 5 ADDITIONAL LEGAL SURVEY

Survey assessing the Member States' rules on health data in the light of GDPR

Additional questions on Business to Business (B2B) and Business to Government (B2G)

According to GDPR Article 20 patients have a right to obtain a portable copy of the data concerning them when such data were collected on the basis of consent or on the basis of a contract and where such data are processed using automated means, and have the right to transmit those data to another controller without hindrance from their original controller. However, Union or MS law may impose restrictions on the exercise of this right in accordance with article 23 GDPR.

1. Please indicate if in your MS any legislation has been adopted that in any way allows a healthcare provider to refuse a request from a patient to transfer data concerning the patient to another data controller?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

   1a. If yes, please describe the situation? In particular, please clarify if such refusal depends on the nature of the other data controller, for example, if data may only be transmitted to another health care provider. Please indicate if any reference is made to limiting rights if data are to be transferred outside the healthcare sector (e.g. to employer or insurer) or outside the MS.

2. In many MS patient records are not based on consent or the execution of a contract but on a legal obligation of a healthcare provider to maintain records, accordingly the right under Art 20 would not apply. However, many MS also have health sector law which grants a right to access to medical records and transfer of medical records. Please indicate if such laws exist in your MS.
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

   2a. If yes, does the law provides for any limitation to such rights, in particular the right to refuse to transfer data to another data controller, despite patient's request to do so? Please provide details on any such limitations.
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

   2b. if yes please provide details of the limitations

3. In some MS legislation exists which obliges a health care provider to release patient data to an insurer. Please describe the situation in your MS.
   - ☐ Yes
   - ☐ Not applicable, not such obligation exists in our health care system

- ☐ Patient data may only be released to an insurer if the patient has consented
- ☐ Health care providers are obliged by law to submit a dataset defined by law to health insurers in order to get reimbursed
- ☐ Other, please specify

4. Can a healthcare provider refuse disclosing health data to insurers?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

   4a. If yes please provide details of the conditions or circumstances that may allow such refusal.

5. Have any sectoral laws been adopted in your MS which address the release of patient data for research purposes?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

   5a. If yes, please describe these laws, in particular if they refer to third party authorisation of the research (eg approval by a research ethics committee) or if they are limited to a particular type of research body (eg publicly financed only)

6. Can a healthcare providers block the release of access to patients' data for research, despite patient's consent that these data can be used for research?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

   6a. If yes, please describe the situation. Is there a difference between the type of researchers who cannot use these data, such as there is only such a possibility to block the transfer to certain types of commercial organisations ?

7. Can a pharma or medical device or other type of company block the release or access to patients' data for research, despite patient's consent that these data can be used for research?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

7a. If yes, please describe the situation. Is there a difference between the type of researchers who cannot use these data, such as there is only such a possibility to block the transfer to certain types of commercial organisations?

7a. If no, please clarify if such data must be anonymised, pseudonymised, or may remain nominative as well as any special rules that may apply.

8. Is there any sectoral legislation in your MS that obliges a healthcare provider (in particular private organisations) to provide patient data to public health authorities for the management of the health care system?

☐ Yes

☐ No

☐ Not sure

8a. If yes, please clarify if such data must be anonymised, pseudonymised, or may remain nominative as well as any special rules that may apply.

8b. Please clarify if such legislation applies also to non-healthcare providers, that is, if a pharma or medical device or other type of company could be obliged to give access to any patient data they hold to a public body for pharmacovigilance or post-market surveillance.

8c. Please clarify if such legislation applies also to non-healthcare providers, that is, if a pharma or medical device or other type of company could be obliged to give access to any patient data they hold to a public body for research purposes.

9. In the original survey you answered questions about data processing for research. Based on feedback from the Commission we would now like to clarify this issue a little further. Please could you clarify if:

9a. Researchers can get access to data held by private companies for research purposes?

☐ Yes

☐ No

☐ Not sure

9b. If yes, does this apply to all types of researchers, or only certain categories, eg publicly funded research organisations or studies? Have any specific conditions been set out?

9c. Please describe the legal basis for such situations

10. Can researchers access anonymised databases of patient information set up by private organisations or professional associations (eg registries of specific associations)
    - ☐ Yes
    - ☐ No
    - ☐ Not sure

10a. If yes, does this apply to all types of researchers, or only certain categories, eg publicly funded research organisations or studies? Have any specific conditions been set out?

10b. What is the legal basis for such situations?

11. Can researchers access information related to clinical trials done by private companies
    - ☐ Yes
    - ☐ No
    - ☐ Not sure

11a. If yes, does this apply to all types of researchers, or only certain categories, eg publicly funded research organisations or studies? Have any specific conditions been set out?

11b. What is the legal basis for such situations?

Thank you for your additional contributions to this study

On behalf of the EUHealthSupport team,
Johan Hansen, Robert Verheij (Nivel, Netherlands institute for health services research), Petra Wilson (Health Connect Partners), Evert-Ben van Veen (MLC Foundation)

Contact: contact@euhealthsupport.eu

GETTING IN TOUCH WITH THE EU

IN PERSON

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

ON THE PHONE OR BY E-MAIL

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone:00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

ONLINE

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU PUBLICATIONS

You can download or order free and priced EU publications from https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en)

EU LAW AND RELATED DOCUMENTS

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

OPEN DATA FROM THE EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

Publications Office
of the European Union

EB-01-21-045-EN-N

ISBN 978-92-9478-785-9