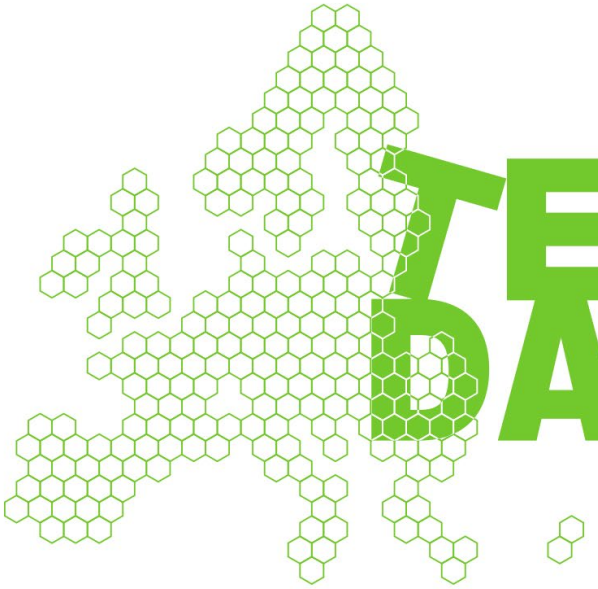

Towards European Health Data Space

Milestone 5.7

Why health is a special case for data governance

23 June 2021

This project has been co-funded by the European Union's 3rd Health Programme (2014-2020) HP-JA-2020-1 under Grant Agreement Proposal Number 101035467.

0 DOCUMENT INFO

0.1 AUTHORS

Author	Partner
Catia Pinto	SPMS - Shared Services of the Ministry of Health, EPE
Coen van Gool	Rijksinstituut voor de Volksgezondheid en Milieu (RIVM)
Fidelia Cascini	Ministero della Salute (MINSAL)
Francesca Marono	Ministero della Salute (MINSAL)
Hannu Hämäläinen	The Finnish Innovation Fund Sitra
Istvan Csizmadia	National Healthcare Service Center (OKFO)
Laszlo Bencze	Semmelweis University (SU)
Leonhard Kamper	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (ATNA)
Marja Pirttivaara	The Finnish Innovation Fund Sitra
Markus Kalliola	The Finnish Innovation Fund Sitra
Tapani Piha	The Finnish Innovation Fund Sitra
Valeria Proietti	Ministero della Salute (MINSAL)
Vincent Sprengers	Rijksinstituut voor de Volksgezondheid en Milieu (RIVM)

0.2 KEYWORDS

Keywords	TEHDAS, Joint Action, Health Data, Health Data Space, Governance

Accepted in Project Steering Group on 22 June 2021.

Table of Contents

1 Executive summary

This document explains why governing health data for its secondary use is a distinct case in the data governance in the European Union. It provides arguments as to why governing health data needs a specific mechanism and cannot be governed by horizontal legislation alone, such as the proposed Data Governance Act.

The digital and data transformation initiative put forward by the European Commission in 2020 provides the springboard for the EU efforts to widen the use of data, including health-related data, in the future. This vision suggests setting up a European Health Data Space (EHDS) as a part of the European data policy. The Member States have supported the proposal, which stems from the General Data Protection Regulation (GDPR).

The GDPR sets out many key concepts, like health data as a special category of personal data as well as genetic and biometric data, which all need special protection. But there is also a broad body of other legislation relevant to the secondary use of health data, which is described in the Annex.

A specific feature in the field of health is that the Member States have a margin to maintain or introduce further conditions as regards the processing of health, genetic or biometric data.

The document puts forward and analyses eight elements, which make health data specific:

1. Patient, consent, and rights of the citizen
2. Protection and promotion of public health
3. Health research and specific data types
4. Health data as highly sensitive data
5. Exceptional need for data and cyber security
6. Health data in the private sector
7. Complex semantic interoperability
8. Fragmented regulatory framework at national level.

An easy-to-read table on each of these elements presents a brief description plus illustrative examples. The arguments as to why the element should be governed by a health-specific mechanism rather than a horizontal mechanism are discussed as is the potential impact of successful governance.

In conclusion, there are important arguments supporting the specificity of health data for its governance in the secondary use and grounds for specific EU legislation. Obviously, the same arguments often apply to the primary use of health data. This unique nature of health data does not lessen the need for the intersectoral use of health data but does underline the necessity for specific safeguards.

This is the first output by the Joint Action Towards the European Health Data Space (TEHDAS). The work on the governance of the secondary use of health data will continue with a study on governance elements, due in August 2021, and to be finalised in a concluding document on governance models for the secondary use of data in the EHDS, due in October 2022.

2 Context

The TEHDAS Joint Action works on various aspects of data governance in a dedicated work package (Work Package 5, WP5). Two documents (called Milestone 5.7 and 5.8) will be produced to underpin the forthcoming legislation on the European Health Data Space.

The first document lays down the foundation of why the specific governance is needed. Once this question has been answered, the rest of the work will deepen the understanding of possible options on how the governance has been currently implemented and what are the possible options going forward.

This document (Milestone 5.7) seeks to respond to two questions:

1. What are the specificities of health data in comparison to data in many other sectors,
2. Why does governing health data in the context of European data spaces require dedicated legislation and a specific European Health Data Space?

These specificities will then point to how the governance of the European Health Data Space needs to be designed. This will be the topic of the subsequent document (Milestone 5.8).

The Commission's proposal for the Data Governance Act (DGA) underlines in Recital (3) that "It is necessary to improve the conditions for data sharing in the internal market, by creating a harmonised framework for data exchanges. Sector-specific legislation can develop, adapt and propose new and complementary elements, depending on the specificities of the sector, such as the envisaged legislation on the European health data space … Specific characteristics of different sectors may require the design of sectoral data-based systems, while building on the requirements of this Regulation".

The scope of the two interrelated documents can be described as follows:

Milestone 5.7 document – What and Why. What are the elements and characteristics ("specificities") of health data, which make the governance of health sector data a specific case? In general, why is specific legislation on the secondary use of health data needed? Could it instead be governed by the proposed horizontal Data Governance Act alone? What added value and new options can be achieved through cross-sectorial use of data based on the Data Governance Act, and what specificities emerge in health?

Milestone 5.8 document - Who and How: Which "design" elements are necessary for structures for the data governance in the health sector? The analysis of existing EU level governance structures, such as the eHealth Network or Data Innovation Board, or those that have only been proposed, provide clues for the necessary governance elements.

The current document provides underpinning elements for the unique nature of health data but makes no recommendations on governance elements and takes no position on the current political discussion regarding data governance or the EU's competency in health.

3 About the work on this document

The format of the document and the framework were chosen to direct the work in a distributed team and to achieve consistent result and to respect the compact size requirements of the final document. What was lost in the breadth and depth of the arguments was gained in readability of the document and keeping with the realistic expectations under the tight timeline for the work. The structure also makes it easy to cut and paste parts of the table for further comparative analysis between elements.

This document is the first policy output from the TEHDAS and its Work Package 5. It starts a series of documents which will jointly form a comprehensive picture of governance options for the European Health Data Space.

This document and the arguments presented in favour for health specific governance can be used as a standalone product to support preparations for the European Health Data Space. It also seeks to promote a wider dialogue about these subjects. However, the main aim of this work is to support the further work in TEHDAS.

This document was created in an iterative process. The kick-off meeting on 22 March 2021 started the process. The scope and objectives were clarified and relation to other work in TEHDAS was taken into account in the planning.

The main work in choosing the elements and drafting the text was done during March-May within the contributors' team in weekly meetings. A larger team of TEHDAS experts convened to give feedback twice in April and once in May.

The first draft was also discussed in a workshop with all TEHDAS partners on 6 May 2021. The workshop built coherence and viewpoints from other TEHDAS work packages for the second draft, which was then put into a written consultation both within the TEHDAS partners and the work package advisory group (WPAG5) on 12 May 2021.

The final draft was placed for TEHDAS quality review process on 25 May 2021. The document will be approved in TEHDAS Project Steering Group.

This document does not cover many topics that will be addressed in other TEHDAS outputs:

- Use cases, best practices or barriers to the cross-border sharing of health data
- National GDPR interpretations and derogations
- Data quality or infrastructure related topics
- Citizens' role or citizen engagement
- Sustainability of the EHDS

4 Legislation relevant to secondary use of health data

In February 2020, the European Commission presented a digital reform package including a Communication on A European strategy for data, notably for policy measures and investments to enable the data economy. The Commission's vision of creating a single European data space by 2030 foresees as legislative key actions a cross-sectoral (horizontal) governance framework for data access as well the establishment of common (sectoral) European data spaces in strategic sectors and domains of public interest including a common European health data space (EHDS). Within the proposed horizontal framework of the common data space, the Commission foresees a legislative framework for the governance of common European data spaces (Q4 2020) and, as appropriate, a Data Act (2021). Regarding the EHDS, the Commission considers sector-specific legislative or non-legislative measures, complementing the horizontal framework of the common data space. In the work programme 2021 the Commission has planned EHDS legislative proposal for Q4/2021.

The Council underlined EHDS in multiple conclusions during 2020. Communication on shaping Europe's digital future from June 2020 underlined the potential of the development of a EHDS which requires a common understanding of the use of health data. In this regard, the Council held already in January 2020 in its position and findings on the application of the General Data Protection Regulation (GDPR) that it is necessary to take data protection aspects and the GDPR fully into account in relevant fields of EU policy and law-making. Later in October 2020 conclusions stated that "The European Council welcomes the creation of common European data spaces in strategic sectors, and in particular invites the Commission to give priority to the health data, which should be set up by the end of 2021."

Open issue

EDPB / EDPS Joint Opinion on DGA 10/03/2021
The joint opinion underlines that "the need to ensure consistency with the GDPR with regard to the competence of the supervisory authorities, the roles of the different actors involved, the legal basis for the processing of personal data, the necessary safeguards and the exercise of the rights of the data subjects". It also raises multiple open questions which need to be discussed in the Council and Parliament during the co-legislation process.

The first main specificity of personal health data from a legal perspective is their qualification as "special categories of personal data" that deserve special protection under the GDPR by way of specific derogations from a general prohibition of processing of such data as well as specific measures to safeguard the fundamental rights and interests of the data subject under the GDPR.

The GDPR, in addition to the legal definitions of "personal data", "processing" and "pseudonymisation", introduced new definitions of "data concerning health", "genetic data" and "biometric data". With regard to the degree of their sensitivity and thus the need for special protection, (sensitive) data concerning health may encompass the subsets of the (even more sensitive) biometric and genetic data. Regarding genetic data, the EDPB only recently pointed out that the possibility to anonymise genetic data remains an unresolved issue but strongly advised to treat such genetic data as personal data. Concerning biometric data, the recently proposed Artificial Intelligence (AI) Act qualifies AI systems intended to be used for the "real-time" and "post" remote biometric identification of natural persons as a High-Risk AI system. Anonymised data, in contrast, are not explicitly but only indirectly defined by the given definitions in the text (as well as recital 26) of the GDPR since it applies only to personal data but not to anonymous information. In this regard, the EDPB repeatedly pointed out that the process of anonymising personal data constitutes a processing of personal data and must therefore be conducted in a manner compliant with the GDPR.

The second main specificity of health data is the margin of the Member States (MS) to maintain or introduce further conditions, including limitations, regarding the processing of genetic data, biometric data or data concerning health, thus modifying the provisions of the GDPR (Art. 9 para. 4 and recital 53). This according to stakeholders and the European Commission has not worked and has created fragmentation. And under Article 9(2) GDPR, there are specific provisions that allow for EU (as well as national) law to complement the GDPR and provide legal basis and further harmonised specifications for processing of special categories of data, including health data, genetic data, and biometric data. However, such harmonization will not negate the need to regulate certain aspects of the secondary use also at national level. For example, DGA does not aim to grant, amend, or remove any of the substantial rights on access to data.

Open issue

The EC data strategy states that "Fragmentation between Member States is a major risk for the vision of a common European data space and for the further development of a genuine single market for data. A number of Member States have started with adaptations of their legal framework, such as on use of privately held data by government authorities, data processing for scientific research purposes, or adaptations to competition law. Others are only starting to explore how to handle the issues at stake. The emerging differences underline the importance of common action in order to leverage the scale of the internal market."

Is there a conflict between EC efforts to harmonize single market for data with further EU legislation, given the MS's legislative margin under Art. 9 para. 4 GDPR which justifies fragmentation?

As an example of MS use of margin for specifying further conditions to the processing of health data the document lists two national legislations in Annex: the Spanish Data Protection Act tackles the use of pseudonymised data in biomedical research1; and a Finnish Act on the Secondary Use of Health and Social Data.2

An overview of legislation related to health data is given in Annex.

1 https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf
2 The Finnish Act on the Secondary Use of Health and Social Data (in English). Ministry of Social Affair and Health. https://stm.fi/en/secondary-use-of-health-and-social-data

5 Why health data is a specific case in legislation?

The following tables describe the most important special characteristics (or elements) of health data that need to be considered in the European legislation on the secondary use of health data. The tables also include examples and give an overview of the bottlenecks and problems observed. They assess why the element needs to be governed by legislation specific to the health sector and the potential impact of the successful governance.

The specificities or elements discussed in the tables are:

1. Patient, consent, and the rights of data subjects i.e. citizens and patients.
2. Public health: Protection and promotion of public health.
3. Research and specific data types, such as genetic and biometric data.
4. Health data as highly sensitive data, and the need for safeguards.
5. Data and cyber security.
6. Health data in the private sector.
7. Semantic interoperability.
8. Fragmented regulatory framework at national level but the need for cross-border sharing.

In particular, elements 1-4, 6 and 8 include strong ethical aspects. The health-specific ethical considerations characterise much of the legislation in the field of health.

6 Elements of health data specificity

6.1 Element 1: The Patient

Element	1
Element name	The patient
EIF	Legal and regulatory level

Description

Governing health data exchange cross-border and internationally should respect natural persons' right to the protection of personal data (TFEU). In the context of health and health care both persons and patients yield health data, which is regarded to be different from data from 'consumers' in other contexts, and therefore their health data should be handled differently.

With the GDPR the EU has signalled the protection of personal health data a fundamental right. Yet, aggregated health information consists of personal health data. And aggregated health information is essentially basic input for research and policy.
At the same time, health data is special in the sense that it pertains a subject with high societal saliency: public health. The sharing of health data and the implied benefits to the wider public, might be the grounds on which the rights of an individual or patient might not prevail.

The EU needs to handle these conflicting interests when developing the European Health Data Space, balancing patient empowerment and the common good on the one hand and the (cross-border re-) use of health data as better steering information for health policy, research, and innovation on the other.

Examples of the element

Patient privacy
Patient consent for sharing and re-use of data,
Patient re-identification versus anonymization of aggregated data

The patient and citizen as co-contributor of scientific efforts and secondary uses of health information through either passive or active participation and information given at the right time in the data processing chain

Patient data in light of GDPR art. 13 to 23, and notably the provisions to restrict certain data subject rights, be it proportionally and in line with fundamental rights and freedoms

Why this element should be governed specifically by the health sector?

While national Member States laws may have specificities on health data protection and since the EU has taken on both patient rights and e-health as priority areas, these should be brought into accordance at an EU wide level when they intersect. Important patient rights, that need to be taken into account when developing e-health initiatives such as the European Health Data Space, include:

- "The right to receive medical care across the border and to have it reimbursed;

- The right to have their personal data protected (in accordance with the GDPR), across the border but on a national level as well;
- The right of access to health data, meaning the right to inspect these data and transfer them to other healthcare organizations;
- The right to receive information, for instance on medical devices via EUDAMED;
- The right to the availability of services that enable the safe exchange of information, like the recognition of electronic identification in Europe." (2)

Potential impact of successful governance

The potential impact of successful governance would imply a certain support base among EU patients and citizens for the cross-border and European exchange of health data. Successful governance would also imply the institution of a regulatory framework to specify under which conditions patients' personal health data can be included in the exchange of aggregated health information in Europe. In addition, it would also imply clear identification of main actors involved and their role as well as establishment of mechanisms and procedures that assess the validity and quality of the sources of the data. Finally, successful governance would imply closer collaboration in the areas of interoperable systems, networked care, and healthcare innovation. Based on mutual agreements, we can develop a health information ecosystem that will be to everyone's advantage, but for the European patients and citizens in particular.

Sources

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/ECArt. - 16 TFEU: Data Protection. Para. 1: Right to protection of personal data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504
2. Elise Peters, Vincent van Pelt. Why Europe? The importance of a joint European approach to information exchange in healthcare. Nictiz. 2021. https://www.nictiz.nl/wp-content/uploads/Paper-Why-Europe-Nictiz.pdf
3. European Data Protection Supervisor. Preliminary Opinion 8/2020 on the European Health Data Space. EDPS. 2020. https://edps.europa.eu/sites/edp/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf

6.2 Element 2: Public health

Element	2
Element name	Protection and promotion of public health
EIF	Legal and regulatory level

Description

Health data is not only used for the benefit of the individual whose data is used but also commonly for the benefit of other individuals and the larger community. This is clear in the case of infectious

diseases, as well as societal or environmental health threats where the use of data is of vital and urgent interest but also when developing prevention or treatment of other diseases. This requires balancing of various interests, in particular public health, and privacy. These public health purposes create a good basis for the acceptance of the secondary use in communities. Cross-border sharing of data can remarkably add to the power of data analysis and use.

Examples of the element

- This is acknowledged in the GDPR as the processing of health data requires a specific justification lifting the prohibition to process such special categories of personal data (Article 9(2)) in addition to the general legal basis (Article 6).
- Recital 159 states that scientific research purposes should also include studies conducted in the public interest in public health.
- Recitals 52-54 already acknowledge the need for processing of special categories of personal data in public health sector.
- COVID-19 highlights the need for effective and rapid data sharing nationally as well as across borders as between players.
- Multi-country medical research on prevention or treatment

Why this element should be governed specifically by the health sector?

- Requires proper understanding of public health aspects of the use of personal, health data in addition to the impact on the individual.
- Can be extremely specific in different situations in the public health.
- The implications of use of personal, health data can be far reaching for an individual but also for the society.
- Will require specific rules and practices on safeguards, not necessarily applicable in other sectors.

Potential impact of successful governance:

- Sharing of health data across jurisdictions becomes easier
- Wider use of health data to control health threats
- More rapid development of new prevention and treatment methods
- Developing the effective and sustainable functioning of healthcare
- Maintaining the trust of citizens. For example, the European Patients Forum is positive towards the aims of the GDPR and subscribe to the use of data for public health purposes but call for guidance on the use and safeguards.

Sources

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

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf
2. The General Data Protection Regulation1 : Secondary Use of Data for Medicines and Public Health Purposes Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures. European Medicines Agency EMA. 2020. http://www.encepp.eu/events/documents/Discussionpaper.pdf
3. The new EU Regulation on the protection of personal data: what does it mean for patients? A guide for patients and patients' organisations. European Patients Forum. Appr. 2018. https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf

6.3 Element 3: Research and specific data types

Element	3
Element name	Research, specific data types (biometric, genomic, and other omics data) and related metadata.
EIF	Legal and regulatory level

Description

Human research data in general and specific types of data such as biometric, genomic, and other omics data coming from current health studies and research, are the knowledge base which allows the practice of medicine and the promotion of health, that now more than ever aim at personalization and precision. Related metadata, i.e. data that accompany and describe data, allow to better understand the context of digital technologies generating research and specific types of data and information to facilitate data management, data sharing and data analysis. Research and specific types of data and metadata are finally essential to understand, anticipate, if not predict the possible occurrence of, and solve, as precisely as possible, diseases (including rare diseases or epidemics), causes of illnesses, risk factors for health, and to predict probabilities of successful therapeutics and standards of care.

Research and specific types of data and metadata can be produced by different healthcare organizations and research institutions and also by: independent non-profit research organizations; private companies developing or marketing health apps (mHealth) and using digital tools to create and collect digital highly sensitive data from research health devices with biometric data/metadata; General Practitioners platforms generating and collecting data/metadata; direct-to-consumer genetic testing companies; crowd-sourcing of health information initiated by citizens, patients cooperatives, independent researchers, citizen scientists, patient-directed researchers, and self-experimenters; private companies belonging to pharmaceutical, medtech, diagnostic and life sciences sectors; AI tools or platforms publishers; health insurance companies.

Examples of the element

Data and metadata regarding test results (biological parameters), clinical records, treatment results (effects), DNA and RNA sequences, protein sequences. Other elements as contents of research projects (video, audio, text, images) or acquired during research activities; surveys and questionnaires responses, transcripts, codebooks as research tools or deliverables; audiotapes, videotapes, photographs, films, images related to research activities.

Why this element should be governed specifically by the health sector?

As a definition, data governance refers to the exercise of authority and control over the management of data. The purpose of data governance is to increase the value of data while minimizing data-related cost (e.g. management, sharing, analysis) and risks related to the human rights violation.

Governing the secondary use of research, biometric, genomic, and other omics data and metadata is fundamental considering the high sensitivity of this type of data and metadata possibly addressing a personalized medicine and bringing individual information also involving relatives.

While there is a possibility to further restrict access to such data vs GDPR at the national level, sector specific rules could create an exception for privacy preserving (nationally) distributed evaluation of clinical, omics, image, and biometric data for R&D and public interest. This could preserve national and EU citizen interest while enabling novel technologies as well as tapping the potential of the EHDS.

Potential impact of successful governance

In general, data governance entails defining, implementing, and monitoring strategies, policies and shared decision-making over the management and use of data assets.

A successful governance of research and specific types of data and metadata, such as those above mentioned, can affect positively - mainly reducing risks for human rights violations at a national and European level - all the healthcare activities such as: providing diagnosis and treatment of diseases, health promotion, adopting prevention programmes, planning distribution of healthcare services, practicing personalized medicine, transforming, and adapting the healthcare systems to new emerging needs.

Further, a successful governance of the secondary use of these data and metadata implies significant socio-economic benefits, coming from the proper use of data to permit faster and safer diagnostics, development of pharmaceutics and pharmacogenomics, advancement of preventive medicine, improvement of health and quality of life for patients, efficient health systems. On the other hand, to have inadequate or suboptimal governance would result in harm in being able to do this, meaning poorer innovation.

Finally, a successful governance of these data is relevant to better manage the complex interplays of various actors and resources involved in health data action areas.

Sources

1. Beyond 1 M Genomes https://cordis.europa.eu/project/id/951724
2. Declaration of genomic cooperation https://digital-strategy.ec.europa.eu/en/news/eu-countries-will-cooperate-linking-genomic-databases-across-borders
3. Data Governance and data Policies https://ec.europa.eu/info/sites/info/files/summary-data-governance-data-policies_en.pdf
4. Health data governance: https://www.oecd.org/health/health-systems/Health-Data-Governance-Policy-Brief.pdf

6.4 Element 4: Health data as highly sensitive data

Element	4
Element name	Health data as highly sensitive data, and the need for safeguards.
EIF	Regulatory framework, governance

Description

Individual right to health and health protection is one of the Human Rights of UN and it is often one of the key pillars on the national constitutional laws. After the EU regulation personal data can be processed only by consent or legislation.

Personal Health data is defined a very sensitive data which includes personal information of health status, Electronic Health Record (EHR), use of health services and treatment Electronic Patient Record (EPR), medication, lab test, images, operations, …. Health data can be stored and processed after the informed consent of patient, legal obligations or after national health service legislation which give the right to store and process the data for health service provider. National legislations often define the responsibilities of service providers/data controllers about the usage of data, and they describe for which purpose it can be processed and what kind of limitations there exist, such as for which purpose the data can be used and in which format.

The concept of health data has widened with bio- and genetic information and personal health and well-being applications are even widening our views on health-related information and data.

The sensitiveness of health data and processing of it are not just regulatory issues.

GDPR and national legislations are giving guidelines and defining demands for the safeguards which are obligatory for health data. Safeguards are the base for the trust of citizens that they can rely on the realisations of their fundamental rights. Level of sensitiveness of health data need special safeguards and demands for it.

The professional secrecy also covers personal data and all facts obtained from or about patients by health care professionals. Professionals subject to professional secrecy are e.g. medical professions, social care, and civil servants. Also researchers using health data for the secondary purposes, like research, development, and innovation, are included in the professional secrecy.

Safeguards for the professionals are unchangeability of EPRs, protecting the professionals, and patients as well. There are limitations of the access to health data. Only care team has right to access the data in the primary use. In the secondary use of health data, the access is limited to those who are permitted, and to specified / limited health data in a safe and secure environment.

Examples of the element

Appropriate GDPR safeguards for international transfers of personal data outside the EU/EEA include:

A legally binding and enforceable instrument between public authorities.
Binding corporate rules (BCRs)
Standard contractual clauses adopted by the local regulatory authority.
Standard contractual clauses adopted by a supervisory authority and approved by the local regulatory authority.
An approved code of conduct.
An approved certification mechanism.

Healthcare specific GDPR related safeguards include e.g. informed consent, pseudonymisation/anonymization/de-identification, encryption, research ethics committee approval, technical and organisational measures ensuring compliance with GDPR. [1]

One example of non-binding recommendations regarding health data is a recommendation by the Council of Europe in 2019, to be applied when health-related data are exchanged and shared. The recommendation has a detailed discussion of health data related safeguards. [2]

Why this element should be governed specifically by the health sector?

According to the GDPR, "Data concerning health" means "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". Data concerning health needs higher protection, as the use of sensitive health data may have significant adverse impacts for data subjects. [3, Recital 53]

The European Data Protection Board (EDPB) states that "data protection safeguards must be embedded in the core of the upcoming EHDS, with the aim of guaranteeing the respect of fundamental rights of individuals, including the right to privacy and to the protection of personal data of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter')." [3]

Potential impact of successful governance

The GDPR safeguards should be integrated with other regulatory safeguards, provided e.g., by competition law, medicines regulatory requirements or ethical guidelines or the coming EU Regulation on AI based on April 21, 2021 draft. [4]

Besides the European solutions, there is a need for global discussion on health data - led by the European Union - to encourage all countries to adopt appropriate privacy and data protection rules and discuss about options for regulatory reform and governance. This is very important for the whole ecosystem. [5] [6]

Sources

1. Assessment of the EU Member States' rules on health data in the light of GDPR. European Union. 2021. https://ec.europa.eu/h https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192 ealth/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf
2. Recommendation CM/Rec (2019)2 of the Committee of Ministers to Member States on the protection of health-related data. Council of Europe. 2019. https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html
3. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. European Data Protection Board (EDPB). 21 April 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf
4. Preliminary Opinion 8/2020 on the European Health Data Space. European Data Protection System (EDPS). 17 November 2020. https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en

5. International Sharing of Personal Health Data for Research. The ALLEA, EASAC and FEAM joint initiative on resolving the barriers of transferring public sector data outside the EU/EEA. All European Academies ALLEA, European Academies Science Advisory Council EASAC, Federation of European Academies of Medicine FEAM, 2021. https://allea.org/wp-content/uploads/2021/03/International-Health-Data-Transfer_2021_web.pdf
6. Tamar Sharon, Federica Lucivero. Introduction to the Special Theme: The expansion of the health data ecosystem – Rethinking data ethics and governance. Big Data & Society July–December 2019. https://journals.sagepub.com/doi/pdf/10.1177/2053951719852969

6.5 Element 5: Data security, cybersecurity

Element	5
Element name	Data security. Cyber security.
EIF	Integrated public service governance / Security and Privacy

Description

Responsible way of secondary use of health data is a health policy imperative to maintain citizens' trust and meaningful investments in data processing. Health data captured in professional systems and provided by citizens can be processed for secondary purposes, and both ways need specific (cyber) security management.

Data subjects also need transparent information how safe the anonymisation or pseudonymisation activities are, while data controllers and data processors need up-to-date guidelines. It is also important that legislation improves the trust of citizens and patients so that they will share their data through the data altruism organisations foreseen in the DGA or other ways of donation or through their care and wellness providers or any other relevant channels. Providers shall take measures to ensure a high level of security for the storage and transmission of non-personal data" as one of the conditions for providing data sharing services. [DGA, Article 11 (8)]

Recommendation 15, which addresses Principle 8 in the European Interoperability Framework, one of the four principles related to generic user needs and expectations, gives guidance to public administrations on how to improve governance of their interoperability activities regarding security and privacy. It suggests to "define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses." Security and privacy are overarching the EIF layers as a fundamental requirement, and therefore, ENISA use cases applies for all layers.

Examples of the element

If consent for primary use of data in the provision of healthcare services, e.g. 1) electronic health/medical/clinical records of diagnosis, treatment, hospitalisation, prevention, rehabilitation, treatment planning and billing; 2) patient-doctor consultation in remote care; 3) measurement results of medical devices (i.a. heartbeat measurements) were supplemented with consent for additional processing purposes through e.g. anonymisation or pseudonymisation, security and privacy issues shall be managed along the whole chain of turning data into value. In this case the weakest links must be treated with special attention by assessing risk factors/impact (confidentiality, integrity, availability) and threat/likelihood (natural phenomena, supply chain failure, human error, malicious actions, system failures). [1] As consent for primary use may not always be an appropriate legal basis for secondary use, other legal bases can be considered as well. For instance, additional uses cases and examples are linked to data altruistic activities when data is not captured in primary data processing environment (e.g. sharing wellbeing data) or data subjects may opt in to sharing data under various appropriate conditions or codes of conduct.
Security risks shall be identified and managed accordingly the weakest link in the chains described by the above examples and use cases.

Why this element should be governed specifically by the health sector?

Security is specific feature of health data, as

- 'Data Saves Life', therefore, changing the content of data sets before analyses and intended or unintended data leakage needs special attention, since damaged or breached data may lead to faults in results of big data analyses;
- Health data is one of the special categories of data (sensitive data);
- Quantum resilience must be considered, since health data can be encrypted and kept confidential for more than 10 years and an attacker could gain access to the ciphertext [2];
- Traceability of medicines and medical devices requires an increased level of security for all actors involved in monitoring;
- Operating and delivering integrated public services / cross-border continuity of care require special attention to improve and maintain level of security;
- The more data digital health (incl. AI, ML) produces and uses, the more interesting it becomes for frauds or breaches, and threat and vulnerability become higher, e.g. ransomware threats.

Therefore, cyber security has special aspects in health data and data systems. They shall be secured (after the death of data subject as well) with special approach from organizational to cross-border levels, e.g. 'Zero Trust Approach' [3]

Potential impact of successful governance
The potential impact of successful governance would:

- increase level of trust
- avoid mistreatment and ineffective innovation
- improve efficiency of secondary (also primary) use of health data

Sources

1. Cloud Security for Healthcare Services. ENISA. January 18, 2021. https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

2. Post-Quantum Cryptography, Current state and quantum mitigation. ENISA, May 03, 2021. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
3. How Hospitals Can Establish a Zero Trust Security Model, Tommy Peterson, healthtechmagazine.net, July 10, 2020: https://healthtechmagazine.net/article/2020/07/how-hospitals-can-establish-zero-trust-security-model

6.6 Element 6: Health data in the private sector

Element	6
Element name	Health data in the private sector
EIF	Legal and regulatory level, governance models

Description

The growing volume of health data and increasing variety of methods to use it for secondary purposes is a growing source for development of new businesses and innovations in personal health, health services, health care management, development of effectivity and quality of health services. National, regional, and local health registries and EHR-systems and the digitalisation of health build comprehensive options to use almost real-time data for industries: health app-developers, health service providers, health and medical technology companies, ICT-companies, pharma industry, insurers, and healthcare platforms. The GDPR allows the use of data for private sector for research purposes. There are a lot of options to use the data for RDI-in a safe and secure way in aggregated or anonymised format to develop health businesses.

Health related industries are not just using the health data, but private health service providers are also producing health care data. Health services are in many EU countries provided by private service providers and therefore they have a lot of data on their patients in EPR's and EHR's. The national health systems vary in Europe: from publicly funded systems to health insurance systems and provision of health services that are semi-public, to totally private systems.

The Data Governance Act separates governance mechanisms and rules for data from public or private sector, but it does not differentiate especially health data provided by public or private sector.

The interests and usage of health data are different in private health services, and pharma, health technology, ICT, or medical devices industries.

Examples of the element
Enlarging health applications business for citizens and health promotion
Decision support systems for health professionals
Value based health care, effectivity of health care and health management
Development of new drugs and medical devices and effectivity of them
Development of personalized medicine and health care
Public health evaluation and planning

Why this element should be governed specifically by the health sector? Permits to use of data for secondary purposes is a health specific issue and should be assessed case by case and processed in health sector by authorities. Public and private Health data are essential for building planning/predictive model, to support decision maker. Health data is very sensitive type of data and therefore privacy and trust are basic elements. Data permit processes must be transparent and base on regulatory framework which define what kind of data can be used to which kind of purpose in private or public interest. Health industry is not just using health data but it is also generating health data. The role of private sector is essential in most parts of health system and therefore both the roles public and private sector should be considered.
Potential impact of successful governance • Increased use of health data in safe and secure environment • Added value for citizens and patient with better and personalised care and medication. • New business opportunities for health-related industries in Member States and Europe • Increased competitiveness of health industry • Better governance and usage of public and private health data
Sources 1. Oderkirk, J. (2021), Survey results: National health data infrastructure and governance, OECD Health Working Papers, No. 127. Paris, OECD Publishing. https://doi.org/10.1787/55d24b5d-en 2. GAIA-X data-infrastructure.eu, see Health. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

6.7 Element 7: Semantic Interoperability

Element	7
Element name	Semantic Interoperability
EIF	Information level
Description Semantic interoperability is how information can be understood and used by all actors for the purpose it is shared. It allows citizens and healthcare providers to interact with each other more efficiently and effectively. It also provides researchers, health authorities and policy makers high quality data for meaningful innovation and insights for policy and regulatory purposes. It is also one of the greatest challenges in health data sharing. The interoperability of health information systems for the different countries is heterogeneous and compartmentalised, especially at the semantic level.	

The present-day health data ecosystem comprises a wide array of complex heterogeneous data sources. A wide range of clinical, health care, social and other clinically relevant information are stored in these data sources. Data may be organised in a proprietary way or be coded using one-of-many coding, classification or terminologies that have often evolved in isolation and designed to meet the needs of the context that they have been developed. This has resulted in a wide range of semantic interoperability issues that make the integration of data held on these different systems a challenging technical endeavour.

The semantic compartmentalisation hinders health data quality and correctness of information for primary and secondary use, which is a pillar of both data protection and healthcare quality.

To overcome obstacles in the consistent application of existing eHealth semantic standards and promote the EU-wide adoption and use of semantic interoperability standards, a dedicated governance framework and strong leadership is required, especially for cross-border sharing of health data.

Examples of the element

Health data is highly heterogenous, encompassing different structured and unstructured data sources, in multiple human and machine languages and in a myriad of data capture systems.

Health Information systems development is shaped by multiple administrative, financial, and legal requirements, deeply rooted in national healthcare systems history and organization. Health data governance cannot overcome this diversity unless it is considered a matter of health policy.

Real world data, patient-generated data and new streams of social media and behavioural data need a strengthened process for data semantic qualification, through scientific advice, for personal health, public health, and health systems improvement purposes.

Personalized medicine further blurs the line between primary and secondary use of health data. Highly complex AI-backed operation of health information systems in patient care will be strictly dependent on the *semantic* quality of the data they hold.

Why this element should be governed specifically by the health sector?

Primary and secondary use of health data need to share the same conceptual data quality requirements; as such, data quality is a matter of healthcare quality, and due consideration for healthcare implications of selected semantic standards is needed. The criticality of the intended use of health data should define the required semantic interoperability standards.

Ensure health-related, sensitive personal data semantic standards are implemented, managed, and reviewed within a technically sound and trustworthy governance framework, that ensures due consideration of specific health data quality requirements, and so, citizens´ health protection rights.

Ensure selection and sustainability of shareable health sector standards under the control of a competent public independent authority.

Potential impact of successful governance Common semantic standards (at EU and national levels) that enable consistent and accurate collection and exchange of health information across health systems and services, irrespectively of the private or public origin of the data capture systems. Agreed semantic metadata management, including development of strategies and cycles that guarantee data can be incorporated, referenced, shared, connected, investigated, and kept up to meet the dynamic and fragmented nature of EU Members States´ healthcare systems.
Sources 1. D8.1 – Report on National eHealth strategies WP8 – Integration in National Policies and Sustainability. eHAction. 2020. http://ehaction.eu//wp-content/uploads/2020/05/13.1_D8.1-Integration-in-national-policies-and-sustainability_eHAction_16th-eHN_ANNEX.pdf 2. Harshana Liyanage, Paul Krause and Simon de Lusignan. Using ontologies to improve semantic interoperability in health data. BMJ Health & Care Informatics. vol 2, Issue 22. 2015. https://www.researchgate.net/publication/280871193_Using_ontologies_to_improve_semantic_interoperability_in_health_data http://dx.doi.org/10.14236/jhi.v22i2.159

6.8 Element 8: Regulatory frameworks at national level

Element	8
Element name	Regulatory frameworks at (sub)national level
EIF	Legal and regulatory level

Description

To date many EU member states have established a national health data governance framework or are in the process of establishing one (Oderkirk, 2021). Far fewer EU member states, however, have embedded these nationwide and centralized regulatory frameworks for the access and re-use of health data in national law. Also, several member states have reported experiencing data governance challenges (Oderkirk, 2021) to developing health data infrastructures: most mentioned were legal or policy barriers to public authorities undertaking data linkages and/or sharing data among public health authorities.

Access to and re-use of (personal) health data nevertheless is common practice in most countries. Many institution-to-institution or within health sector procedures exist for the access to and exchange of health data, especially in country border regions where health institutions need to cooperate with institutions on the other side of the border. These collaborations and (cross-border) exchanges of data may be governed by subnational regulations or even lower governance structures. This causes fragmentation and hampers the unambiguous access and exchange of health data, which in turn proves the need for a more unified regulatory framework.

Examples of the element

The existence of a governing body in a member state.

The level a governing body is acting (national – regional; implications for level of jurisdiction?). The intensity of the regulatory measures that such bodies might adopt (low-medium-high in line with Commission classification?). In turn, strongly related to the more general output of the body. The institutional constellation of the body (notably the management board and voting rights). In turn, strongly related to the more general input of the body (accountability?). Regulatory interplay/competition with other parties, e.g. other governmental and non-governmental rule-making institutions/initiatives. The existence of a national health data strategy (or vision/mission); The regulations stipulated under the (sub)national framework that specify access to (personal or aggregated) health data; specifying under what conditions and to what kinds of data (Hansen et al. 2021)): Conditions: health sector specific procedures for (trusted) access and exchange of health data in place (such as data altruism vs explicit consent) Kinds of data: (aggregated) electronic health record data, disease registry data, research databases, administrative data sources that feed into secondary use of health data (Hansen et al. 2021).
Why this element should be governed specifically by the health sector? Governing health data exchange at supranational level should consider the existing (sub)national regulatory frameworks, outlining who can access the nationally available health data. The mere fact that these national regulatory frameworks apply to (personal) health data only is reason enough to have this element apply to the health sector specifically. There is an opportunity to have more consistency in health data governance across the EU to deal with applicable standards as well governance bodies and authorization of access where not individually consented.
Potential impact of successful governance Successful governance might imply more harmonization of the (sub)national regulatory frameworks. The potential impact of successful governance would also imply less administrative burden for institutions because of promoting recording data only once and facilitate re-use. This principle – together with the yet to be specified concept of data altruism to serve the common good – could act as an accelerant for accessing and (re-) using health data easier, more unified, faster, yielding higher quality data for research and policy.

Sources

1. Johan Hansen et al. Assessment of the EU Member States' rules on health data in the light of GDPR. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf
2. Jillian Oderkirk. Survey results: National health data infrastructure and governance, OECD Health Working Papers, No. 127. Paris, OECD Publishing. 2021. https://doi.org/10.1787/55d24b5d-en

7 Annex. EU legislation relevant to secondary use of health data

This Annex complements Chapter 3 on legislation relevant to secondary use of health data. EU tertiary law (e.g. COM delegated or implementing acts) that must be compliant with EU secondary and primary law is not covered by this document.

I. EU law in force

I.1. Primary EU law

Treaty on the Functioning of the European Union (Consolidated version 2016), OJ C 202, 7.6.2016.

- Art. 16 TFEU: Data Protection.
  - Para. 1: Right to protection of personal data.
  - Para. 2: EU rules relating to the protection of individuals regarding the processing of personal data and the free movement of such data.
- Art. 114 TFEU: Approximation of laws.
  - development based on scientific facts.
- Art. 168 TFEU: Public Health.
  - Para. 1: High level of human health protection shall be ensured in definition and implementation of all Union policies and activities.
  - Para. 7: MS' responsibility for definition of health policy and organisation and delivery of health services and medical care including management of health services and medical care and allocation of resources assigned to them.
- Art. 179 TFEU: Research
  - Para. 1: EU's objective of achieving a European Research Area.
- Art. 191-193 TFEU: Environment
  - Art. 191 para. 1: EU policy on environment shall contribute to (…) protecting human health.
  - Art. 192 para. 1: Action is to be taken by the Union in order to achieve the objectives referred to in Art. 191.
  - Art. 193: MS may maintain or introduce more stringent protective measures that must be compatible with the Treaties.
- Art. 338 TFEU: Statistics

Charter of Fundamental Rights of the European Union (2016), OJ C 202, 7.6.2016; primary law according to Art. 6 para. 1 of the Treaty on European Union (Consolidated version 2016), OJ C 202, 7.6.2016.

- Art. 7 of the Charter: Respect for private and family life.
- Art. 8 of the Charter: Right to protection of personal data.
- Art. 24 (The rights of the child)
- Articles 51-54 (Title VII: General Provisions Governing the Interpretation and Application of the Charter)

I.2. Secondary EU law

Related to primary data use and governance

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45–65.

Legal basis: Art. 114 (esp. para. 3) TFEU + Reference to Art. 168 (incl. para. 7) TFEU.

Most relevant provisions: Chapter IV (Art. 10-15), esp. Art. 14 on eHN (voluntary in compliance with Art. 168 para. 7 TFEU).

Currently under evaluation in the COM expert group 'Fit for Future Platform' and evaluation of Art. 14 as part of the regulatory gap study commissioned to Open Evidence Consortium.

Related to primary and secondary data use as well as governance

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection

Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88 ("GDPR").
Legal basis: Art. 8 of the Charter + Art. 16 TFEU.
Most relevant provisions: All incl. Art. 4, 5, 6 and 9 (cf. recitals 46 and 51-56), esp.

- Art. 4 (Definitions) paras. 1 ('personal data'), 2 ('processing') and 5 ('pseudonymisation'); cf. recitals 26-30.
- Art. 4 (Definitions) paras. 13 ('genetic data'), 14 ('biometric data') and 15 ('data concerning health'); cf. recitals 34 and 35.
- Recital 26 on pseudonymous and anonymous information: The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person using additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.
- Art. 6 para 3-4
- Art. 9 para. 2 lit. j icw Art. 89 (cf. recitals 156-163),
- Art. 9 para. 4: MS' margin to maintain or introduce more specific provisions to adapt the application of the rules of the GDPR (Note: in case of conflict with recital 53 last sentence, the legal text prevails over the non-binding recital),

Chapter III (Rights of the data subject),
Chapter IV (Controller and processor),

- Section 2 (Security of personal data),
- Section 3 (Data protection impact assessment and prior consultation),
- Section 5 (Codes of conduct and certification) and

Chapter VI (Independent supervisory authorities) and Chapter VII (Cooperation and consistency).

- Council position and findings on the application of the General Data Protection Regulation (GDPR), 14994/2/19 REV 2, 15 January 2020:
  - Recital 42: "The Council notes the risk of fragmentation of legislation relating to the margin the Member States have to maintain or introduce more specific provisions to adapt the application of the rules of the GDPR. While that margin has been intentional

for the specification of certain provisions of the GDPR and a certain fragmentation is therefore justified, the Council considers that the developments in this respect should be followed closely. In addition, the Council considers it necessary to take data protection aspects and the GDPR fully into account in relevant fields of EU policy and law-making."

- Council conclusions on shaping Europe's digital future (2020/C 202 I/01), OJ C 202I, 16.6.2020, p. 1–12:
  - Recital 43: "[The Council] UNDERLINES that the development of a European Health Data Space by the Commission together with the Member States' health authorities holds potential to facilitate the development of effective prevention, diagnosis, treatments and care. It may also ensure more cost-effectiveness and workflow optimisations in health care, thus leading to improved health outcomes for patients, better epidemiological surveillance systems, and longer-term sustainability of health systems. AGREES that the European Health Data Space should be purpose- and quality-driven. This requires a common understanding of the use of health data in accordance with international, Union and national law, and in full compliance with the specific high-level requirements for the protection of personal health data."

Related to primary and secondary data use as well as governance

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons regarding the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance), OJ L 295, 21.11.2018, p. 39–98 ("EUDPR").

Legal basis: Art. 8 of the Charter + Art. 16 TFEU.
Most relevant provisions: All incl.

- Art. 10 (Processing of special categories of personal data),
- Art. 13 (Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) and
- Chapter VI (Art. 52-60): European Data Protection Supervisor and Chapter VII (Art. 61-62): Cooperation and Consistency.

Related to GDPR and EUDPR

Regulation (EC) Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (Text with EEA relevance), OJ L 354, 31.12.2008, p. 70–81.

Legal basis: Art. 338 TFEU (ex Art. 285 TEC).
Art. 3 lit c: Definition of 'public health' (cf. Art. 9 para. 2 lit. i and recital 54 of the GDPR; also applies for EUDPR).

Related to GDPR

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/EC (Text with EEA relevance), OJ L 158, 27.5.2014, p. 1–76.
Legal basis: Art. 114 TFEU + Art 168 para. 4 lit. c TFEU (measures setting high standards of quality and safety for medicinal products and devices for medical use).

Most relevant provisions:

- Chapter V (Art. 28-35): Protection of subjects and informed consent (to participation in scientific research activities in clinical trials; cf. Art. 89 and recital 161 of the GDPR).
- Art. 41-43: Legal basis (legal obligation) for controllers to process personal data in clinical trials for reliability and safety related purposes.

Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (Text with relevance for the EEA and for Switzerland), OJ L 87, 31.3.2009, p. 164–173.

Legal basis: Art. 338 TFEU (ex Art. 285 TEC).
Most relevant provisions:

- Chapter V (Art. 20-26): Statistical confidentiality (cf. Art. 89 and recital 163 of the GDPR).

Related to data protection and governance

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.), OJ L 117, 5.5.2017, p. 1–175.
Regulation (EU) 2020/561 of the European Parliament and of the Council of 23 April 2020 amending Regulation (EU) 2017/745 on medical devices, as regards the dates of application of certain of its provisions (Text with EEA relevance), OJ L 130, 24.4.2020, p. 18–22.
Legal basis: Art. 114 TFEU + Art 168 para. 4 lit. c TFEU (measures setting high standards of quality and safety for medicinal products and devices for medical use).

Most relevant provisions:

- Art. 33 (European database on medical devices).
- Art. 62 (General requirements regarding clinical investigations conducted to demonstrate conformity of devices and Art. 63 (Informed consent).
- Chapter VIII (Art. 101-108): Cooperation between Member States, Medical Device Coordination Group, Expert Laboratories, Expert Panels and Device Registers.
- Art. 109 (Confidentiality) and Art. 110 (Data protection).

Related to data security

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73-114.
Legal basis: Art. 114.
Most relevant provisions:

- Chapter II (Art. 6-12): Electronic identification.
- Chapter III (Art. 13-45): Trust services.

Related to data protection but not specifically health

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37-47.

Legal basis: Art. 114 TFEU (ex Art. 95 TEC) + Reference to Art. 7 and 8 of the Charter.
Art. 1: Particularising and complementing the GDPR (as a lex specialist) with respect to processing of personal data in electronic communication sector and to ensure the movement of such data and electronic communication equipment and services.
No health-specific provisions.
Proposal for a Regulation on Privacy and Electronic Communications, 10.1.2017, COM (2017) 10 final.

Related to non-personal data

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance), OJ L 303, 28.11.2018, p. 59.

Legal basis: Art. 114 TFEU.
Art. 2 para. 2: “In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.”
Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 172, 26.6.2019, p. 56-83.

Legal basis: Art. 114 TFEU.
Art. 1 para. 4: “This Directive is without prejudice to Union and national law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC and the corresponding provisions of national law.”

Regulation (EU) 2018/1807 and Directive (EU) 2019/1024 related to non-personal data:
Anonymising personal data constitutes processing of personal data under Art. 4 para. 2 GDPR (cf. EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, adopted on 2 February 2021, para. 43 on p. 11).

Possibility to anonymise genetic data remains an unresolved issue. However, EDPB strongly advises to treat such genetic data personal data (cf. EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, adopted on 2 February 2021, para. 50 f. on p. 12).

Related to health data security and governance

NIS Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.
Legal basis: Art. 114 TFEU.
Most relevant provisions:

- Art. 4 para 4 (operator of essential services; cf. recital 28) icw Annex II (5. Health sector: Healthcare providers as defined in Art. 3 lit. g of Directive 2011/24/EU).
- Chapter III (Art. 11-13): Cooperation.

Proposal for a revised NIS Directive (NIS2), 16.12.2020, COM (2020) 823 final.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), OJ L 151, 7.6.2019, p. 15–69.

Legal basis: Art. 114 TFEU.
Most relevant provisions:

- Title II (Art. 3-45): ENISA (The European Union Agency for Cybersecurity), esp. Chapter II (Art. 5-12): Tasks (cf. recitals 1 and 15: Health) and
- Title III (Art. 46-65): Cybersecurity certification framework.

Related to accessing genetic resources

Regulation (EU) No 511/2014 of the European Parliament and of the Council of 16 April 2014 on compliance measures for users from the Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization in the Union (Text with EEA relevance), OJ L 150, 20.5.2014, p. 59–71.

Legal basis: Art. 192 para. 1 TFEU.
Article 2 (Scope):

- Para. 2: Regulation does not apply to genetic resources for which access and benefit-sharing is governed by specialised international instruments that are consistent with, and do not run counter to the objectives of the Convention and the Nagoya Protocol.
- Para. 3: Regulation is without prejudice to Member States' rules on access to genetic resources over which they exercise sovereign rights within the scope of Article 15 of the Convention, and to Member States' provisions on Article 8(j) of the Convention concerning traditional knowledge associated with genetic resources.

Most relevant provisions (related to health):

- Recital 16: Pandemic Influenza Preparedness Framework for the sharing of influenza viruses and access to vaccines and other benefits (the 'PIP Framework') constituting a specialised international access and benefit-sharing instrument.
- Art. 4 (Obligation of users) para. 8: Imminent public health emergency of international concern within the meaning of the International Health Regulations (2005) or a serious cross-border threat to health as defined in the Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC (OJ L 293, 5.11.2013, p. 1).

Proposals to include digital sequence information on genetic resources can be found from the United Nations Convention on Biological Diversity[3].

I.3. EU secondary law under development

Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act) (Text with EEA relevance), 25.11.2020, COM (2020) 767 final.

[3] Digital sequence information on genetic resources. Convention on Biological Diversity. United Nations. 2021. https://www.cbd.int/dsi-gr/

Related to EHDS as a proposed horizontal data governance framework.

Foreseen legal basis: Art. 114 TFEU.
Recital (3) provides that "This Regulation is therefore without prejudice to Regulation (EU) 2016/679" – in contrast to:
EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), adopted on 10 March 2021, para. 25 on p. 8 f.:

"EDPB and EDPS consider that ***the Proposal raises significant inconsistencies with the GDPR****, as well as with other Union law, in particular as regards the following five aspects:*

(a) Subject matter and scope of the Proposal;
(b) Definitions/terminology used in the Proposal;
(c) Legal basis for the processing of personal data;
(d) Blurring of the distinction between (processing of) personal and non-personal data (and unclear relationship of the Proposal with the Regulation on free flows of non-personal data);
(e) Governance/tasks and powers of competent bodies and authorities to be designated in accordance with the Proposal, having regard to the tasks and powers of data protection authorities responsible for the protection of the fundamental rights and freedoms of natural persons in relation to the processing of personal data as well as for facilitating the free flow of personal data within the Union."

Proposal for a Data Act (scheduled for 2021)
Potentially related to the EHDS.
Granting, amending, or removing the substantial rights on access and use of data.
Cf. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, 19.2.2020, COM (2020) 66 final.

Commission documents related to Artificial Intelligence

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future, 19.2.2020, COM(2020) 67 final:

- Key action: White Paper on Artificial Intelligence setting out options for a legislative framework for trustworthy AI (adopted together with this Communication), with a follow-up on safety, liability, fundamental rights, and data (Q4 2020).

White paper on Artificial Intelligence - A European approach to excellence and trust, 19.2.2020, COM (2020) 65 final.

Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence, 21.4.2021, COM (2021) 205 final.

- P. 8 f.: The 2021 review of the coordinated plan is an opportunity to generate further European added value and strengthen the global role of the EU on AI. It puts forward four key sets of suggestions on how the European Commission, together with Member States and private actors, can accelerate, act, and align to seize the opportunities AI technologies offer and to facilitate the European approach to AI. These four key sets of suggestions are

described here below. (…) Fourth, advance in building strategic leadership in high-impact sectors[31], including climate change and the environment, health, the public sector, robotics, mobility, security and home affairs, and agriculture.

- FN 31: This is in addition to the horizontal action areas that build on the action areas proposed in the 2018 coordinated plan.

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21.4.2021, COM(2021) 206 final.

Foreseen legal basis: Art. 16 and Art. 114 TFEU.
Recital (45): (…) For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent, and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing, or supporting the access to data may also support the provision of high-quality data for the training, validation, and testing of AI systems.

P. 13: 5.2.3. HIGH-RISK AI SYSTEMS (TITLE III):
Title III contains specific rules for AI systems that create a high risk to the health and safety or fundamental rights of natural persons. In line with a risk-based approach, those high-risk AI systems are permitted on the European market subject to compliance with certain mandatory requirements and an ex-ante conformity assessment. The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. Therefore, the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used.

Strong focus on ‘biometric data’:

- Art. 3 (Definitions) paras. 33 (cf. recital 7) – 38.
- ANNEX III: High Risk AI Systems referred to in Article 6(2):
- Para. 1 (Biometric identification and categorisation of natural persons) lit. a: AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons.

A European Health Data Space – Legislative proposal Q4 2021 – Combined evaluation roadmap / Inception Impact Assessment (Ref. Ares (2020)7907993 - 23/12/2020).

Directly related to EHDS:
Foreseen legal basis: “Articles 114 of the Treaty on the Functioning of the European Union, potentially combined with other Article 16 on data protection, could provide the legal basis for this action.”

However, since this evaluation/assessment also covers “primary use of health data” and even recognises that “the organisation and financing of the health sector requires a specific approach on digital health technology”, the lack of any explicit reference to Art. 168 para. 7 TFEU seems to be insufficient from a legal as well as political point of view.

II. Member States' national laws

II.1. General

1. National laws regulating the definition of health policy and organisation and delivery of health services and medical care including management of health services and medical care and allocation of resources assigned to them in accordance with Art. 168 para. 7 TFEU.
2. National transpositions of the various opening clauses under the GDPR including (but not limited to) Art. 9 para. 4 of the GDPR.
3. National implementation of relevant EU laws mentioned in this document.

Further analysis of Member States' national laws under the GDPR will be performed later by the TEHDAS Joint Action.

II.2. Spain: Example on the use of pseudonymised personal data in biomedical research

Organic Law 3/2018, of December 5, of Protection of Personal Data and guarantee of digital rights.
Extract from Additional Provision 17ª.2.: "Re-identification of data at origin may take place when, in the course of 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".

II.3. Finland: Example on national implementation of Art. 9 GDPR and data security requirements for a "safe processing environment"

Act on the Secondary Use of Health and Social Data (552/2019).
Deals with national derogations under Art. 9 GDPR
Source: the Finnish Ministry of Social Affairs and Health, Finland[4]

Chapter 4 (Sections 35-42): Justifications and preconditions to the secondary use of personal information:

- Section 39 (Education): Art. 9 para. 2 lit. g of the GDPR.
- Section 40 (Planning and reporting duty of an authority): Art. 9 para. 2 lit. g of the GDPR.
- Section 41 (Knowledge management): Art. 9 para. 2 lit. h of the GDPR.
- Chapter 5 (Sections 43-54): Processing of a data permit application, a data request, and the data to be disclosed:
- Section 43 (General grounds for granting a data permit): General reference to GDPR.
- Section 45 (Processing of a data request): Art. 9 para. 2 lit. g and Art. 86 of the GDPR

Regulation by the Health and Social Data Permit Authority Findata (1/2020): Requirements for other service providers' secure operating environments.
Deals with data security requirements for a "safe processing environment"
Source: Findata[5]

[4] Secondary use of health and social data. Ministry of Social Affairs and Health. Finland. 2021. https://stm.fi/en/secondary-use-of-health-and-social-data
[5] Findata has issued a regulation on the requirements of secure operating environments. Findata. 27.10.2020. https://www.findata.fi/en/news/findata-has-issued-a-regulation-on-the-requirements-of-secure-operating-environments/

Legal basis: Act on the Secondary Use of Health and Social Data (552/2019), Section 22(3) and Section 24(2).
Information security requirements refer to the following provisions and criteria:

- Act on the Secondary Use of Health and Social Data (552/2019), Chapter 3 (Sections 10-34): Services than enable secondary use.
- KATAKRI 2015 - Information security audit tool for authorities.
    - The KATAKRI Protection level and/or sections in the Example must be considered in the application, if any are presented.
- PiTuKri version 1 March 2020 - Criteria to Assess the Information Security of Cloud Services.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- ISO/IEC 27001 standard.