European Commission

DG Health and Food Safety

Country fiches for all EU MS

Annex to the study '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 978-92-9478-786-6 doi:10.2818/09448 EB-01-21-048-EN-N

Country fiches for all EU MS

Annex to the study '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 Eline Verhoeven[1], Madelon Kroneman[1], Petra Wilson[2], Mary Kirwan[3], Robert Verheij[1,4], Evert-Ben van Veen[5], Johan Hansen[1] (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

1 COUNTRY FICHE BELGIUM 5
2 COUNTRY FICHE BULGARIA 11
3 COUNTRY FICHE CZECHIA 18
4 COUNTRY FICHE DENMARK 28
5 COUNTRY FICHE GERMANY 39
6 COUNTRY FICHE ESTONIA 48
7 COUNTRY FICHE IRELAND 56
8 COUNTRY FICHE GREECE 63
9 COUNTRY FICHE SPAIN 73
10 COUNTRY FICHE FRANCE 82
11 COUNTRY FICHE CROATIA 93
12 COUNTRY FICHE ITALY 100
13 COUNTRY FICHE CYPRUS 109
14 COUNTRY FICHE LATVIA 114
15 COUNTRY FICHE LITHUANIA 124
16 COUNTRY FICHE LUXEMBOURG 130
17 COUNTRY FICHE HUNGARY 137
18 COUNTRY FICHE MALTA 145
19 COUNTRY FICHE THE NETHERLANDS 152
20 COUNTRY FICHE AUSTRIA 158
21 COUNTRY FICHE POLAND 166
22 COUNTRY FICHE PORTUGAL 174
23 COUNTRY FICHE ROMANIA 179
24 COUNTRY FICHE SLOVENIA 185
25 COUNTRY FICHE SLOVAKIA 191
26 COUNTRY FICHE FINLAND 197
27 COUNTRY FICHE SWEDEN 204
28 COUNTRY FICHE UNITED KINGDOM 212

1 COUNTRY FICHE BELGIUM

The following sections provide an overview of the rules for processing of health data currently in place in Belgium both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[1]

1-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	**Loi du 22 août 2002 relative aux droits du patient** concerns the contractual and the non-contractual relationships between the patient and the healthcare professional and describes the legal basis on which health or care providers and health or care professionals can process health data for direct in-person care of the data subject and patients' rights. **Loi sur les hôpitaux, coordonnée le 7 août 1987, Article 17 novies** regulates patients' rights. It makes a direct link between this legislation and the one described above, in order to apply patients' rights in the context of hospitals. **Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Article 9** describes the specific measures to be put in place when health or care providers (processors) process health data.
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent • 6(1)(c) legal obligation + 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	**Loi du 22 août 2002 relative aux droits du patient** concerns the contractual and the non-contractual relationships between the patient and the healthcare professional and describes the legal basis on which health or care providers and health or care professionals can process health data for direct in person care of the data subject and patients' rights. **Loi sur les hôpitaux, coordonnée le 7 août 1987, Article 17 novies** regulates patients' rights. It makes a link between this legislation and the one desctibed above, in order to apply patient rights in the context of hospitals. **Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé , Article 36 to 40,** which regulates the access to health data by healthcare providers or professionals. **Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Article 9** describes the specific measures to be put in place when health or care providers (processors) process health data.

[1] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Belgium. The authors of the report take full responsibility for any interpretations in the country fiche.

	Arrêté royal du 3 mai 1999 relatif au dossier médical général (D.M.G.) and **Arrêté royal du 3 mai 1999** amended by **Arrêté royal du 16 avril 2002 portant fixation des normes minimales générales auxquelles le dossier médical,** as referred to in Article 15 of the **Loi sur les hôpitaux, coordonnée le 7 août 1987** applies.
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent • 6(1)(c) legal obligation + 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Belgium has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 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
Specific legislation on **genetic testing**	
National legislation	Belgium has specific regulations for genetic testing. The legislation is: 4 DECEMBRE 1987 - Arrêté royal fixant les normes auxquelles les centres de génétique humaine doivent répondre. and **Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Article 9** which describes the specific measures to be put in place when genetic data is processed.

1-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Belgium has no specific legislation on this topic.
Specific legislation addressing 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.	
National legislation	Belgium has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Belgium has no specific legislation on this topic. **Note. Loi sur les médicaments du 25 mars 1964, Article 3, §1, second alinea** which states that a specific Arrêté royal can be adopted to define the specific rules for the processing of health data that was originally collected for the purpose of providing care to allow it to be used for pharmacovigilance. **This specific Arrêté royal** (execution measure of the Law) has **not yet been**

	adopted at the time drafting this report (December 2020)..
Specific legislation addressing 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**	
National legislation	Belgium has no specific legislation on this topic. A specific legislation for the Corona virus pandemic is currently being elaborated and should be adopted by end Q1 20212021.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Not sure.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
National legislation	Belgium has not adopted specific legislation at national level on this topic.
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	**Loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions,** which relates to the creation of the eHealh platform and access to health data it contains. **Loi du 25 février 2018 portant création de Sciensano, Article 4, § 4,** which relates to the collection of health data in the framework of public health, and the creation of disease registries (notably the registry for rare diseases).
Legal basis GDPR	• 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
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • A healthcare professional may be given access to the data that he or she has submitted to the registry • 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 • Public sector researchers • Private researchers

* Note. 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.

1-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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	Belgium has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) – but

different controller than that where the treating healthcare professionals were based.	requiring the data to be de-identified or pseudonymised for a secondary use) • Explicit consent is the default legal basis 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
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.	Belgium has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised for a secondary use) • Explicit consent is the default legal basis 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
National legislation	Since the entry into force of the GDPR, the conditions for the re-use of health data for scientific or historical research are regulated by the GDPR (Articles 9 and 89) supplemented by **Article 9 of the Loi du 30 juillet relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,** while other provisions of this Law (i.e. **Articles 186 to 208)** aim at creation of specific derogations to the data subjects rights in order to facilitate scientific or historical researches. The legislation does not differentiate between not for profit researchers and for profit researchers. Hence, the legislation in place is for both public and private researchers jointly.

1-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Belgium the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Belgium:	
Mechanism	• Application to a local research ethics committees • The data controller provides direct access upon proof of agreement of a research ethics committee or DPA • Other: Application to Information Security Committee (sectoral body). This is not an ethical evaluation that has to be done by an ethical committee.
Sectoral law on health data: **Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE** The legislation covers the communication of personal data concerning health except: • Between health professionals involved in the care of a particular patient • Scientific research where the following conditions are cumulatively met: o the persons concerned gave their explicit and informed consent to participate in the scientific research before any personal data is communicated to the investigator(s);	

○ the persons concerned are selected in an appropriate manner; ○ the data are obtained directly from the data subjects; ○ personal data are not communicated to third parties; ○ the principles of information security are respected; (in all these circumstances, only the articles of the GDPR apply) • Anonymous data
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project
Belgium did not adopt such a system.
Legislation has been adopted 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
Belgium has no specific legislation on this topic.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
Belgium has adopted a system to facilitate this. The platform that facilitates the re-use of EHR data for research is Healthdata.be.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Belgium has no specific legislation on this topic.
Data access infrastructure 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: https://www.ehealth.fgov.be/fr

1-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Belgium.

Rights of the patient	How the right can be exercised in Belgium
Article 15 'right to access data concerning him or her'	• Through a formal national data access request system established by legislation
Loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions, Article 6 which states that: *« La présente loi ne porte nullement atteinte à la loi du 22 août 2002 relative aux droits du patient ».* This means that the patient should require access to his/her medical information through his/her GP as provided for in the law of 22 August 2002, by direct reference to Article 15 GDPR. This is still possible in Belgium. However, the eHealth platform now contains the EHR of each patient which can be accessed through the use of the identity card of the patient, a specific tool for the card and some numerical keys.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Belgium has not adopted specific health data legislation on Article 16.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
Belgium has not adopted specific health data legislation on Article 17.	

Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

1-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Belgium to include data from apps and devices in the EHR. In addition, the table displays how Belgium has adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
• This is organised nationally. https://www.masante.belgique.be/#/	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	These mechanisms differ from one care institution to another. There is therefore no uniform response to this question.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Belgium does not yet participate in eHDSI but plans to do so by 2025.	
Technical standards	
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	
Policy level	• 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) • 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)
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

1-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	eHealth platform
Hospital and medical specialist care	This is regionalized in Belgium. One example in the Wallonia Regio: https://www.reseausantewallon.be/FR
Prescription drugs	**Recip-e (e-prescription platform)**

2 COUNTRY FICHE BULGARIA

The following sections provide an overview of the rules for processing of health data currently in place in Bulgaria both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[2]

2-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	Pursuant to Article 5 of the Personal Data Protection Law, health data can be processed only under the conditions and for purposes provided by law. Health information falls, altogether, under the scope of PDPA. General data protection regime is therefore applicable to health information together with the specific rules of the Health Act, which further develop and complement it. The National Health Insurance Fund (NHIF) and health practitioners in Bulgaria fall in the legal definition of 'administrator of personal data' (Administrator) and as such are subject to the Personal Data Protection Law's requirements. Administrators cannot begin collecting, hosting and processing personal data before being officially registered by the Commission for Personal Data Protection. The Commission controls` Administrators' compliance of personal data protection requirements and can impose mandatory instructions on them.
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	**Bulgarian Health Act, Section 5, article 27** enables specified health care providers and health professionals to collect, process, use and store health information (paragraph 2 and 3). Article 28(1) regulates when health information may be provided to third parties. Article 28(2) states that "the provision of information in the cases under par. 1, item 2 shall be carried out after notifying the respective person." Article 28(3) states that "The persons under art. 27, para. 2 shall be obliged to ensure protection of the health information stored by them from illegal access."
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent • 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Bulgaria has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
National legislation	Bulgaria has no specific legislation on this topic.

[2] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Bulgaria. The authors of the report take full responsibility for any interpretations in the country fiche.

Specific legislation on **genetic testing**	
National legislation	Bulgaria has specific regulations for genetic testing. ORDINANCE No. 38 of 20.08.2010 on the approval of medical standard "Medical genetics". Section 1, art. 2 provides requirements for medico-genetic consultation, organization and operation of laboratories, recommended methodologies for laboratory work and principles to ensure quality of genetic research, as well as the creation of a National Genetic Laboratory and national genetic register. Article 141 and 142 and the following Health Act governs genetic research and examinations of the human genome for medical and scientific purposes. In order for any kind of processing to commence, the data controller needs to apply for registration with the PDPC (Art. 17 PDPA). In case the processing will involve health and genetic data, the Personal Data Protection commission (PDPC) will carry out a mandatory preliminary check prior to registering the controller and the respective processing (Art. 17b, para. 1 PDPA). The check is performed within 2 months of the application submission (Art. 17b, para. 2 PDPA). The controller shall not commence the processing prior to being registered with the PDPC. Under current Bulgarian legislation a researcher may collect health data directly from individuals only provided the individual has given his/her consent (Art. 5, para. 2, pt. 2 PDPA). The individual's consent should be express, specific and informed, and, as per our understanding, it should be provided in written form. The consent may be withdrawn at any moment. Additionally, Chapter 7, Section IV of the HA (Art. 197 and following HA) entitled "Medical research upon persons. Medical science" contains provisions regarding the organization, control and responsibilities in the field of medical and science research upon individuals.

2-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	The Regulations for the Organization and Activity of the National Center for Public Health and Analysis, issued by the Ministry of Health, Prom. DV. issue 54 of July 17, 2015, amended and ext. DV. issue 82 of 18 October 2019, amended and ext. DV. issue 89 of 12 November 2019, regulates the structure and activity of the National Centre. The NCPHA is a structure of the national healthcare system. Article 1(3) specifies in what activities the NCPHA assists the Minister of Health: research, assessment of health risks, health promotion and disease prvention, and information provision of the healthcare management.
Legal basis GDPR	• 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
Specific legislation addressing 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.	
National legislation	The Medical Wares Act Article 1(1) regulates the conditions of medical devices and obligations of manufacturers, as well as the supervision on the market and the incident

	notification system. Article 1(2) (Amended, SG No. 38/2015, effective 26.05.2015) sets out the purpose of the Act, which is 1. to ensure the placing on the market and / or putting into service of medical devices which do not endanger the life and health of patients, medical professionals or third parties, when the devices are used for their intended purpose and are stored, distributed, installed, implant and maintain in accordance with the manufacturer's instructions; 2. to ensure the implementation of Commission Implementing Regulation (EU) No 920/2013 by 24 September 2013 on the designation and monitoring of notified bodies under the Directive Council Directive 90/385 / EEC on active implantable medical devices and Directive Council Decision 93/42 / EEC concerning medical devices (OJ L 253/8 of 25 September 2013), hereinafter referred to as "Implementing Regulation (EU) No 920/2013". The **Ordinance No 9 of 1 December 2015 on the Conditions and Procedure fr Performance of Health Technology Evaluation**, issued by the Minister of Health, Prom. DV. issue 97 of 11 December 2015, revoked. DV. issue 26 of March 29, 2019. Article 1(1-4) regulates the conditions and the order for carrying out assessment of health technologies (HTA).
Legal basis GDPR	• 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
Specific legislation addressing 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**	
National legislation	Bulgaria has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Bulgaria has no specific legislation on this topic.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. It is regulated by Ordinance № 21 of 18 July 2005 on the Procedure for Registration, Communication and Reporting of Infectious Diseases.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	Bulgaria has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	The legal basis of disease registries stems from the initial decision to create and regulate the NCPHA, which is regulated by the Regulations for the Organization and Activity of the NCPHA. In addition, the Ministry of Health Ordinance No 16 of July 30, 2014 on 'The terms and conditions for registration of rare diseases and for centers of expertise and reference networks for rare diseases' addresses rare disease registries.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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 • 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

* Note. 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.

2-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Bulgaria has no specific legislation on this topic.
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.	Bulgaria has no specific legislation on this topic.

2-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Bulgaria the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Bulgaria:	
Mechanism	• Application to a centralised data governance and access body (hence other than each data controller / data custodian individually)
The National Center Of Public Health And Analyses (NCPHA) provides statistical information following the Health Act (HA) and the Personal Data Protection Act. The provision of access to public information by the NCPHA is carried out on the basis of a written application or an oral inquiry in accordance with the Internal Rules for Ensuring Access to Public	

Information in the NCPHA and the Access to Public Information Act (APIA).
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project
Bulgaria did not adopt such a system.
Legislation has been adopted 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
To our knowledge, there is no legislation that specifically considers the FAIR principles.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
Bulgaria did not adopt such a system. Pursuant to Article 27(3) of the Health Act, the form and content, as well as the terms and conditions for the processing, use and storage of medical information and the exchange of medical statistical information shall be determined by ordinance of the Minister of Health, coordinated with the National Statistical Institute. The ordinance will have to specify the general rules on archiving duration of health records, the destruction of records, the automatic transfer of health data for statistical purposes and the type of health data that can or cannot be used for such purposes. However, no such general ordinance has been adopted yet.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Bulgaria has no specific legislation on this topic. Currently, Bulgarian legislation does not provide for a specific regime for the setting up and the use of private databases with health data for research purposes. While creating a private database containing health data is not prohibited, its legal basis must be carefully applied. The processing of health data is in principle prohibited, therefore the setup of a private database with health information would need to be carried out provided that data subjects have given their explicit consent (exception to the prohibition of processing sensitive information under Art. 5 para. 2, pt. 2 Personal Data Protection Act (PDPA). Under the current framework, the setup of a private database with health information may be performed only after a mandatory check-up has been carried out by the Personal Data Protection Commission - PDPC and the owner of the database is registered with the PDPC as data controller.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
There are no official entities through which researchers can share or access data from EHRs.

2-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Bulgaria.

Rights of the patient	How the right can be exercised in Bulgaria
Article 15 'right to access data concerning him or her'	• Through a formal national data access request system established by legislation
National Health Act, Section 2, Art. 86, para. 13 states that as a patient, one has the right to access the medical records related to his health condition.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a formal national data rectification request system established by legislation
Bulgaria has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten'	• No, a patient may not delete his or her medical

May a patient have medical records deleted?	record
Bulgaria has not adopted specific legislation on the application of such a right in the area of health.	
Article 20 'right to data portability'	• Through a formal national data portability request system established by legislation

2-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Bulgaria to include data from apps and devices in the EHR. In addition, the table displays how Bulgaria have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
A platform (not a specific institution) for electronic Health Patient Records, supported by the National Health Insurance Fund (NHIF), currently exists. The Health Patient Record contains information on the health status of mandatorily health-insured citizens (immunizations, hospitalizations, medical and laboratory examinations, etc.) as well as information on the general medical practitioner chosen by them. It is accessible through the website of the NHIF with an electronic signature or a personal code issued by the NHIF.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs. Patient generated data is not regarded as an authentic medical data, equal to the data which a health professional may constitute; hence it is not permitted to include such in EHR. On the other hand, patient generated data may serve as indication and ground for further analysis, but not as original health information to be incorporated in the record.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Bulgaria does not yet participate in eHDSI but plans to do so by 2025.	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability
Health Ministry has no official strategies. However, the PIS records are centralised in one database hosted by the NHIF. There are no legal obligations to develop interoperability of PIS records with other systems in Bulgaria, as these records are an initiative of the NHIF. All systems related to the NHIF are interoperable by using the same file format ('xml'). The systems of all NHIF Partners (hospitals, individual health practitioners, pharmacies) are adapted to this format and the Partners also send their monthly or daily medical care reports to the NHIF in xml format. The entire information is centralised in the Internet Information System of the NHIF and relevant information for health insured individuals is automatically extracted and updated in PIS records.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
The Law does not specify what technical standards are applied, but indicates, that they should	

follow the GDPR such as: pseudonymisation, encryption, etc. According to Art. 66 of the Personal Data Protection Act, (1) Administrators processing personal data, taking into account the achievements of technological progress, the costs of implementation and its nature, the scope, context and objectives of the processing, as well as the risks for certain rights and freedoms, should apply appropriate technical and organizational measures to ensure protection in accordance with security risk, in particular the processing of category "personal data" related to art. 51, para 1.
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
Policy level • No, there are no national or regional policies to ensure use of quality standards for health data.
Agencies which oversee the implementation of technical standards
There is no institution or agency overseeing the implementation of technical standards.

2-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	National Center Of Public Health And Analyses (NCPHA) https://ncpha.government.bg/en/
Prescription drugs	Bulgarian Drug Agency (BDA) https://www.bda.bg/en/

3 COUNTRY FICHE CZECHIA

The following sections provide an overview of the rules for processing of health data currently in place in Czechia both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[3]

3-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	Act No. 372/2011 Coll., on Health Services and on Conditions of their provision the "**Health Services Act**") sets general rules for providing of health care in the Czech republic (e.g. definition and types of health care, authorisation for providing of health care, rights and duties of patients and healthcare professionals, medical records, medical confidentiality, establishment of National Health Information System, evaluation of quality and safety of health care, public control of heathcare providers, tresspases etc.). Article 2 para 4 defines what is understood as healthcare. Regarding processing of health data Article 53 para 1 sets the obligation of healthcare providers to keep medical records and use them in accordance with this Act. Article 53 para 2 sets the obligatory general content of medical records and refers to implementing **Decree No. 98/2012 Coll. , on Medical Records,** including health data in Article 53 para 2(d). This Decree sets detailed content of various parts of medical records, as well as the periods for which medical records must be stored at the health care provider. Act No. 89/2012 Coll., **The Civil Code** regulates the storage of medical records in Articles 2647 to 2650. It is a very general regulation compared to the detailed rules in the Health Services Act and Decree No. 98/2012 Coll., on Medical Records.The Civil Code applies as lex generalis for regulating legal relations between the healthcare provider and the patient when processing health data. Its direct application on health services provided under the Health Services Act is therefore limited. However the Civil Code deals with certain topics which are not covered by the Health Services Act, such as the sharing of anonymised patient data for population health statistics (Art. 2650). Act No. 373/2011 Coll., **Specific Health Services Act** regulates the provision of specific health services not covered by the Health Services Act, such as assisted reproduction and genetic testing. Act No. 374/2011 Coll., **Emergency Medical Services Act** regulates provision of emergency medical services. Act No. 378/2007 Coll., **Pharmaceuticals Act** sets rules for the development, production, distribution, use, control and disposal of pharmaceuticals. It regulates rules for Clinical Trials of human medicinal products. This Act also sets out the E-Receipt information system, see below.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	

[3] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Czech Republic. The authors of the report take full responsibility for any interpretations in the country fiche.

National legislation	The Health Services Act, Art. 51 para 2 sets exceptions from the general obligation on medical confidentiality. The healthcare provider can share information on the patient (including health data) with other healthcare providers for purposes of ensuring continuity of health services. Consent of patient is not required in this case.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	There is no specific legislation for processing of health data when providing digital health services. However there are some partial regulations: the Pharmaceuticals Act and **Decree No. 329/2019 Coll., on Prescription of Pharmaceuticals during Healthcare Provision**; and the Health Services Act. The Pharmaceuticals Act describes the E-Receipt information system in art. 81 para 1. This public administration information system is administrated by the State Institute for Drug Control. The E-Receipt information system consists inter alia of the Central Repository of Electronical Prescriptions and the Patient's Medication Record. • E-prescriptions Doctors are obliged to issue all prescriptions in electronic form since 01.01.2018 pursuant to art. 80 of the Pharmaceuticals Act. Cross-border e-prescription is not available yet but it is expected that it shall be within two years. E-prescriptions are stored for a period of 5 years since its creation and deleted from the Central Repository of Electronic Prescriptions after this period. • Patient's Medication Record The shared electronical patient's medication record is established by art. 81d of the Pharmaceuticals Act and is implemented since 01.06.2020. Doctors providing health care and pharmacists providing medication to patients will have access to data stored in the patient's medication record. The access to patient's medical record is based on the opt-out principle (e.g. presumed consent if the patient does not express disagreement) and serves mainly for purposes of providing healthcare as well as patient's safety (preventing of undesirable medication interaction). • Patient summary Article 56a of the Health Services Act deals with another digital health service: the patient summary. Healthcare providers may decide whether they want to create and store patient summary or not (it is voluntary). It is part of the medical documentation and contains basic information on the health condition of the patient and provided health services. The purpose of its creation is cross-border sharing of basic health data between healthcare providers from different EU MS for the purpose of providing health care. A patient summary can be shared based on a request by a healthcare provider/professional addressed to the National Contact Point, administrated by the Ministry of Health. Data are securely shared through eHDSI. • E-sick leave From 01.01.2020 e-sick leave has been introduced pursuant to Act No 589/1992, on Social security and State employment policy premiums, and Act No 187/2006, on sickness insurance. It is an electronic system for processing Decisions on temporary incapacity to work (containing also health data – information that the employee is temporarily incapable to work. Communication between the physician, employer and also Social Security Administration is electronical in the information system.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	Czechia has specific regulations for genetic testing. The **Convention on Human Rights and Biomedicine** (Oviedo Convention) sets general rules for providing predictive genetic testing – it can be provided only for health purposes or for scientific research connected with health purposes, and also for genetic consulting. The **Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes** came into force on 01.09.2019 in Czech Republic. It sets more detailed rules on providing genetic testing for health purposes (it does not cover genetic testing for research).

	Rules for ensuring quality when providing of genetic testing are set in article 5. Article 28 para 3 of the Specific Health Services Act states that genetic testing can be provided only by a provider authorised by a public authority to provide health services in field of medical genetics (e. g. Medical Genetics Provider, Clinical Genetics Provider and Laboratory of clinical genetics). Laboratories providing genetic testing must have a valid certificate of accreditation for providing genetic testing by the Czech Accreditation Institute (according to the ISO norm – now CSN EN ISO 15189). Furthermore, the Specific Health Services Act sets purposes for which genetic testing can be provided, sets that genetic testing can be provided after written consent is given by a patient, sets rules upon which genetic counseilling is recommended to a patient and his relatives, and sets rules upon which biological material gained when providing health care can be used for genetic testing.

3-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Health Services Act Article 70 establishes the National Health Information System (NHIS), the unified system administred by the Institute of Health Information and Statistics of the Czech Republic (Statistics Institute, IHIS), organisational unit of state established by the Ministry of Health. Art. 70 para 1 states inter alia that NHIS is intended for processing data in the health sector in order to obtain information on the scope and quality of the health services, for the management of the health sector, for the creation of health policy, assessing quality and safety indicators of health services etc. Pursuant to art. 70 para 2 NHIS contains personal data of patients (to the extent set in art. 70(2)(a)); health care providers (natural persons) (to the extent set in art. 74(1)); and health care professionals (to the extent set in art. 76(1)). This data is transmitted to NHIS without the data subjects' consent unless stated otherwise in the Health Services Act. The legal basis for transmission of personal data to NHIS and for processing personal data in NHIS for purposes set by legislation is therefore not consent. These data are transmitted to NHIS by persons defined in art. 70 para 4, such as providers and health insurers.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation addressing 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.	
National legislation	Act No. 48/1997 Coll., **Public Health insurance Act** governs mainly the public health insurance system in Czech Republic and the scope and conditions pursuant to which healthcare services are covered from public health insurance. Art. 39d of this Act states that the State Institute for Drug Control can, in the public interest, decide on temporary reimbursement of so called highly innovative products for which there are insufficient data on the cost-effectiveness or therapeutic outcomes when used in clinical practice. Art. 39d para 7 states that healthcare providers who

	submit these highly innovative products are obliged to provide data related to the efficacy assessment and the status of the highly innovative product in clinical practice to a health insurance company and, in anonymized form, to the holder of the registration decision for the medicinal product. The scope of the data (including health data) transmitted to the health insurance company and the holder of the registration decision for a highly innovative product is set by art. 42 of **Decree No. 376/2011 Coll**., that implements selected provisions of the Public Health Insurance Act. Health Insurance Companies have established the Health Insurance Bureau (HIB), a private association, and empowered HIB (inter alia) to process data on highly innovative products pursuant to the Public Health Insurance Act and Decree No. 376/2011 Coll. Collected data can be used for further proceedings – e.g. prolongation of temporary reimbursement or decision on "permanent" reimbursement by The State Institute for Drug Control.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	**Pharmacovigilance** Art. 90 of Pharmaceuticals Act sets rules for the pharmacovigilance system of Czech Republic which is in compliance with EU legislation – Directive 2010/84/EU. The pharmacovigilance system is operated by the State Institute for Drug Control ("Institute") and is intended to: a) collect information on the risks of human medicinal products as regards patients' or public health b) evaluate the information as per (a) and consider options for minimisation and prevention; c) adopt measures consisting where necessary Pursuant to art. 91 of this Act the marketing authorisation holder is obliged to operate the pharmacovigilance system. Art. 93a para 2 sets the obligation to report to the European EudraVigilance database in case of suspected serious and non-serious adverse reactions. Art 93b of the Pharmaceuticals Act regulates the reporting by healthcare professionals to the Institute when they noticed a suspected serious or unexpected adverse reaction and other facts that might affect the health of the treated persons in association with the use of a medicinal product. The scope of personal data reported are set in art. 15 para 1 and 3 of **Decree No. 228/2008 Coll., on Registration of Pharmaceuticals**. Only pseudonymised data in the sense of GDPR are being reported to the Institute. **Medical devices** Art. 69 of the Medical Devices Act regulates the Vigilance system which is a system of reporting and evaluation of adverse incidents and safety corrective actions regarding medical devices. Art. 70 of this Act sets obligation to report a) to the Institute by the manufacturer or authorised representative; and b) the obligation to report to the Institute and manufacturer by the importer, distributor, provider of healthcare services, servicing person, dispensing person and seller. Art. 70 para 3 sets out what data should be reported. There is no explicit request for reporting personal data directly in the Medical Devices Act. However suspected adverse incidents are reported via electronic form with content set by **Decree No. 62/2015 Coll.** The Manufacturer is obliged to investigate suspected adverse incident and send final report in structure set by art. 71 para 3 of the Act. The Institute reviews this report and informs the Commission and the concerned authorities of the Member States about measures adopted or considered by the manufacturer.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

Specific legislation addressing 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**	
National legislation	The Public Health Protection Act regulates the epidemiological surveillance of selected infectious diseases. Art. 75a sets a national system of epidemiological surveillance which is set for infections named in this Act and in **Decree No. 473/2008 Coll., on Surveillance System for Selected Infectious Diseases** (such as measles, influenza etc.) Art. 75a para 4 states that care providers are obliged to collect and report data on selected infectious diseases in structure set by Decree No. 473/2008 Coll. and report them to the regional hygiene station (public health authority) through the Information System of Infectious Diseases administrated by the Statistics Institute. Hygiene stations are obliged to collect data on reported infectious diseases and provide the data to the Ministry of Health pursuant to art. 75a para 2 of the Act. The Ministry of Health is responsible for transferring data on reported infectious diseases to The European Surveillance System (TESSy). For infectious diseases not included in the surveillance system the general rule in the Public Health Protection Act applies – the healthcare provider is obliged to report findings on infectious diseases or suspicion on infectious diseases to the regional hygiene station and then act pursuant to orders of the regional hygiene station. Processing of personal data by public health authorities and providers are regulated in: • Art. 47b of the Act enables public health authorities to use data from state information systems such as the population register • Art. 54 of the Act states that healthcare providers are obliged to report to public health authority personal data of a person who is carrier of an infectious disease named in art. 53 (such as HIV/AIDS, typhoid fever etc.). • Art. 79 para 1 of the Act explicitly states that public health authorities are obliged to process these personal data for purposes of fulfilling its obligations connected with protection and promotion of public health. • Public health authorities are also entitled to process personal data on employees doing risky work defined in art. 39 para of the Act.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
No, it is not possible.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	Art. 70 para 1 of the Health Services Act states that **National Health Registers** (e.g. disease registries) are part of NHIS. There are 12 National Health Registers which form a mutually interconnected system within the NHIS where it is possible to collect aggregate data for the purposes specified in Health Services Act. All Health Registers are private and only accessible for persons specified in legislation except for the National Register of Providers which is available for the public (with exception of some personal data). Access to the various registers is specified in the Health Services Act: National Health Registers: Art. 73(2); National Register of Providers and National Register of Healthcare Professionals: Art. 73(2)(c); National Register of Providers: Art. 74(3); and National Register of Healthcare professionals: Art. 76(2). The Statistics Institute can also provide data from the National Health Registers for statistical and scientific purposes. Data can be provided only in anonymous form - e.g. form from which no specific natural person or legal entity can be identified. Art. 78 of the Health Services Act and **Decree No. 373/2016 Coll., on Transmission of Data**

	to the National Health Information System stipulate details on providing data to Health Registers, such as entities who transfer data to health registers and the procedure of transfer data to health registers. Act No. 258/2000 Coll., **Public Health Protection Act** regulates the Information System of Infectious Diseases created pursuant to art. 79 para 2. Art. 79 para 3 of the Act states that data from this registers can be used in anonymous form by public health authorities or National Institute of Public Health for purposes of preparing health policy, evaluation of state of support and protection of public health and for monitoring trends of infectious disease occurence . There are also registers connected with donation of tissues or organs and with transplantation created pursuant to Act No. 285/2002 Coll., **Transplantation Act**. A list of other registries than National Health Registries can be found here.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • A healthcare professional may be given access to the data that he or she has submitted to the registry • Public sector researchers** • Private researchers** ** Only anonymous data can be provided based on a request and reimbursement of costs must be provided to IHIS.

* Note. 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.

3-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Czechia has no specific legislation on this topic.
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.	Czechia has no specific legislation on this topic.
National legislation	Czech Republic does not have specific legislation regulating the processing of data collected for purposes of treatment of patients for other purposes such as scientific research. However, those partial rules are relevant: Art. 73 para 8 of the Health Services Act states that data collected in National Health Registers can be provided by the Statistics Institute for scientific and statistical purposes based on request, only in the form from which no specific natural person or legal entity can be identified. Furthermore the Health Services Act deals with using human body parts removed during the provision of health services (such as tissue) for research purposes in art. 81. The patient should give demonstrable consent (this is not consent pursuant to GDPR).

	Act No. 110/2019 Coll., **Processing of Personal Data Act** does not contain specific rules for processing of health data Art. 16 para 1 specifies safeguards referred to in art. 89 of GDPR that are necessary when processing personal data (including health data) for scientific or historical research or statistical purposes. Furthermore the Methodical document on implementation of GDPR on science data (not authoritative guidance) mentions multiple legal bases as possible, e.g. explicit consent, broad consent, public interest in the field of public health and research purposes. Therefore the legal basis used by researchers may differ depending on key characteristics of the research; such as the nature of the research institution (public or private), research purpose (e.g. public or private interest) etc.

3-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Czechia the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Czechia:	
Mechanism	• Other: Patients' consent • Other: Application to the Statistics Institute
There is no specific regulation on access to health data for research. In order to access health data in medical records a patient's consent is needed. The Health Services Act does not allow anyone to access medical records for research purposes without patient´s consent. The law does not set other obligations such as approval of an review ethics committee (REC), DPA or public authority etc. On 1.9.2020 the **Additional Protocol to the Convention on human rights and biomedicine, concerning biomedical research**, entered into force in Czech republic ("Additional Protocol"). The Additional Protocol does not regulate access to health data for research directly but it states that every research project involving intervention on humans shall be submitted to an ethics committee for review. In practice, a description of the processing of health data is part of a research project protocol. Regarding interventional research projects the (legality of) access to health data for research will be often reviewed by an independent REC established by the subject carrying out research (university, hospital). Regarding non-interventional projects (for example retrospective analysis of data) the REC will not be obligatory however in projects carried out by public institutions (universities, public hospitals) there will also be an independent REC, scientific board or similar independent body. Also patient´s consent to participation in a research project is required by the Convention and its Additional Protocol (if it is not a retrospective analysis of data of deceased person). The appropriate legal basis for processing health data for research purposes must also be found by the researcher before accessing the data (e.g. explicit consent, legitimate interest, public interest, public health protection, scientific research). Regarding access to data in National Health Registers, Art. 73 para 8 of the Health Services Act stipulates that the Statistics Institute can provide anonymous data from the National Health Registers for statistical and scientific purposes. The Statistics Institute is entitled to request payment covering the costs related to the acquisition of excerpts, copies, the provision of technical data carriers and the sending of data. Reimbursement for extremely extensive data searches can also be requested.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Czech Republic did not adopt such a system. However, there are several biobanks established, often as part of healthcare providers or universities. Patients can consent with the storage of biological material and data gained during provision of health services (leftovers) in biobanks for the purpose of research. See below more details on this data infrastructure (BBMRI-CZ).	
Legislation has been adopted 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	

Czech Republic has no specific legislation on this topic.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
The NHIS, as explained above, is created also for the purpose of health research (pursuant to § 70 (1)(e) of the Health Services Act). However, access to registries for research purposes is limited as researchers can only access anonymous data.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Czechia has no specific legislation on this topic.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
There are several systems for sharing data for secondary use, administered by separate ICT vendors or service providers. There is no centralized data access infrastructure in the Czech Republic as there is no national regulation on the use of health data for research. However in this context a national node of BBMRI-ERIC (European Research Infrastructure Consortium) – BBMRI-CZ is established. Networks of individual biobanks operate within this consortium (there is no centralised system). Biobanks are often established as organisational part of healthcare providers or universities. Samples of biological material obtained from associated healthcare providers are stored in biobanks (long-term or short- term storage). Patient can consent with this storage. Samples and data can be searched and requested with the use of BBMRI-ERIC's Sample/data locator and negotiatior.

3-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Czechia.

Rights of the patient	How the right can be exercised in Czechia
Article 15 'right to access data concerning him or her'	• Other: Patients can request access to their data kept in medical records by reference directly to art. 65 para 1 of the Health Services Act which is „lex specialis" to GDPR.
The Health Services Act Art. 65 para 1 states that a patient can view his/her medical records in presence of medical staff, and can make copies and excerpts from this documentation. There is a special regime for authorised psychological methods. If a patient does not make an excerpt nor a copy by his own means on the spot, the provider is obliged to make a copy or excerpt of the medical records within 30 days of a request pursuant to art. 66 para 1 of Health Services Act. There is no national data access request system. Patients adress their requests directly to healhcare providers. Healthcare providers can be fined by authorities who issued them authorisation for provision of healh care if they fail to enable the patient to exercise this right of access to medical records (for example art. 117 para 3 of Health Services Act).	
Article 16 'right to rectify any inaccurate data concerning him or her'	• The right to rectification is restricted based on sectoral legislation adopted in accordance with Article 23(1)
The Health Services Act and Decree No. 98/2012 Coll., on Medical Records apply. Art. 54 para 2 states that the medical records, including their independent components, must be kept in a conclusive, true, legible and continuous manner. Pursuant to art. 54 para 4 the corrections of entries in the medical records are made by a new entry. The entry is provided with the date of the correction and signature of the healthcare professional who made the entry. The original entry must remain legible. Addition or correction of the entry in the medical records at the patient request must indicate the date and time of the entry	

and the note that it is a correction or addition made at the patient's request. This entry is signed by the patient and by the healthcare professional.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
The Health Services Act sets obligation of healthcare providers to lead and keep medical records about every patient. Decree No. 98/2012 Coll., on medical records sets periods for which medical records must be stored by the healthcare provider. Medical records must not be deleted before this period ends. Periods can be prolonged (but not shortened) under conditions set by the Decree.	
Article 20 'right to data portability'	• Other: Patients can obtain a portable copy of medical records by reference directly to art. 65 para 1 of the Health Services Act which is „lex specialis" to GDPR.
The Health Services Act Art. 65 para 1 states that a patient can view his/her medical records in presence of medical staff, and can make copies and excerpts from this documentation.	

3-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Czechia to include data from apps and devices in the EHR. In addition, the table displays how Czechia have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
In the E-Receipt information system patients have access to all electronic prescriptions. From 01.06.2020 patients will also have access to the electronical patient's medication record which is also part of the system. A patient's medication record contains a list of all medication prescribed and handed in to patient and names of doctors who prescribed and pharmacists who issued the medication.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so No legislation explicitly forbids healthcare professionals to incorporate patient generated data into EHR so it should be considered as legal. However pursuant to art. 54 para 2 of the Health Services Act a healthcare provider is obliged to keep medical records in a conclusive, true, legible and continuous manner. Medical records also serve as evidence in case of conflict between a provider and patient. The healthcare professional bears the responsibility that data in medical records are correct and it is his responsibility to decide whether and how to use patient generated data for purposes of providing healthcare.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Czech Republic participates in eHDSI through sharing summary records. Article 56a of the Health Services Act deals with the patient summary, as described in 3-1.	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability

In Czech Republic technical standards for interoperability are not defined by legislation. Pursuant to the proposal of the **Act on Electronisation of Health Care**[4] the Ministry of Health Care shall issue standards of electronic health care after consultation with Statistics Institute.

Technical standards used in Czech Republic are for example:

- Standard NCP used in NIX-ZD is the project for developing of cross-border exchange of health data – for example sharing of patient summary.
- National standard DASTA in version 4 (DS4) issued by the Ministry of Health Care which is used for communication with IHIS – providing data to National Health Registers.
- international standard HL7 (Health Level 7) is used for exchange of heath data between software applications of healthcare providers.

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• No, there are no national or regional data security policies to ensure use of standards for data security.

Partial rules are: Art. 55 of the Health Services Act outlines several rules on electronic medical records which must be fulfilled when a healthcare provider desires to keep medical records only in electronic form. Art. 54 para 3 of Health Services Act stipulates conditions under which entries to electronic medical record are made.

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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.

There is no specific health data quality policy, partial rules are:

Section 54 para 2 of the Health Services Act stipulates that medical records must be led in true, legible and conclusive way. This rule applies both for paper and electronic medical records.

Art. 54 para 3 of the Act states that any entry into medical records kept in electronic form it shall be provided with the entry identifier; the entry itself shall contain the unchangeable, undisputable and verifiable data. Para 4 states that the corrections of entries in the medical records shall be made by a new entry. The entry shall be provided with the date of the correction and the other particulars pursuant to Paragraph 3. The original entry must remain legible.

In future (if proposal Act on Electronisation of Health Care will be approved in current version) the standards shall be issued by Ministry of Health Care.

Agencies which oversee the implementation of technical standards

As there are currently no legally recognised technical standards to be overseen. If the above mentioned proposal act will be approved this might change.

3-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data Hospital and medical specialist care	National Health Registers https://www.uzis.cz/index-en.php?pg=nhis--national-health- registers
Prescription drugs	ePrescription application - note that this is not secondary use in sense of the GDPR; since it is (currently) not allowed to access data in patient's medication record for other purposes than providing of health services. https://pacient.erecept.sukl.cz/suklerp/Account/Login?ReturnUrl=%2fsuklerp%2fPacient%2f
Self measurements	No state or state funded app is available. There can be apps developed by private companies but it is not part of Czech E-health system yet.

[4] Please note that the proposal is in process of review and can be substantially changed or dismissed.

4 COUNTRY FICHE DENMARK

The following sections provide an overview of the rules for processing of health data currently in place in Denmark both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[5]

4-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	Consolidated Act no. 903 of 26/08/2019 (**Health Act**) provides a legal framework for the provision of health care services (health promotion, health prevention and treatment) at national, regional and local level, and for the rights of patients and obligations of the health care services. The Health Act includes a number of provisions of particular importance for data processing. Patients' right to privacy is recognized (section 40), and access to and disclosure of health data within the health care services for the provision of care and other related purposes (e.g. quality assurance and administrative and planning purposes) is comprehensively regulated (section 41-42e). To some extend these provisions differ from the GDPR, especially because patients are granted more extensive rights to consent and to object to the sharing of data for provision of patient care. The Health Act also includes provisions regarding patients' right to self-determination in regard to the tissue samples stored in clinical biobanks (section 29-35). Consolidated Act no. 731 of 8 July 2019 on authorization of health care professionals and on health care services (**Act on Authorisation**) includes a duty of health care professionals (section 21-25) to keep and register health data in patient records. This obligation is further specified in Executive Order no. 530 of 24/05/2018.
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	According to the Health Act, sharing of health data among healthcare professionals for the purpose of providing health care to patients require – as a main rule – the patient's informed consent (section 41.1). However, there are a number of exemptions. In situations where it is necessary to disclose health data from one health care professional to another for the provision of care in an actual and specific treatment context, this can be done without the patient's specific consent, provided it is necessary and considered to be in accordance with patient's interests and needs (section 41.2.1). If the other health care professional has direct access to the data – e.g. through an electronic system (EHR) – he/she can have relevant access to the data, if this is necessary and considered to be in accordance with patient's interests and needs. The

[5] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Denmark. The authors of the report take full responsibility for any interpretations in the country fiche.

	difference between the two situations (disclosure vis-a-vis access) is, that in the disclosure situation, the primary health care professional is responsible of not disclosing more information than necessary for the health care professional taking over, whereas in the direct access situation, the accessing health care professional will inevitably get access to more information than necessary when looking into a patient's EHR. The Health Act also authorizes that the patient's medical history (epicrises) can be send from the hospital to the patient's GP (section 41.2.3-41.2.4), and in case the patient is not able to consent to treatment, it is also allowed to disclose or access information if it is of vital interest for the patient (section 41.2.4 and section 42a.2). In some of the situations mentioned above, the patient is entitled to object to the sharing of data.
Legal basis GDPR	• 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Denmark has no specific legislation on this topic. In general, it is mostly GDPR and the Danish Data Protection Act, which provide the regulatory framework for the use of apps in the health care services. But the provisions in the Health Act regarding access to and disclosure of health data also applies, once the data from an app enters the health care services. Furthermore, professional duties and responsibilities also applies to health care professionals recommendation of using specific apps and for relying on data from such devises.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	As there is no specific regulation targeting this kind of data processing, it means that the general rules in the GDPR, the Danish Data Protection Act, and potentially also the Health Act (and the Act on Authorisation) will apply. The potential legal basis for processing of data through apps and other devices are listed below, but the exact legal basis depends on the concrete situation.[6] • 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
Specific legislation on **genetic testing**	
National legislation	Denmark has specific regulations for genetic testing. A National Genome Center (NGC) was established in 2018 through an amendment to the Health Act (Act no. 728 of 08/06/2018). The purpose was to create a national infrastructure as part of a national strategy on personalised medicine. Section 223-223b in the Health Act creates the legal basis for the NGC (section 223) and authorises the NGC to make genetic sequencing in connection with diagnostic and treatment of patients, and to store the genetic information in a national genomic database. In addition, it gives the Minister of Health authority (section 223a) to issue a regulation regarding the obligation of health care institutions and professionals to report genetic information and other health data to the NGC in order to support its tasks and activities. Such regulation follows from Executive Order no. 360 of 04/04/2019. Section 223b lays down more specific rules regarding the processing of health data at the NGC. It is only allowed to process health data for the purpose of preventive health care, diagnostic and treatment and administration of health care services. In addition,

[6] See the legal analysis by Associate Professor, PhD, Hanne Marie Motzfeldt, published as an appendix to a report from the Danish Council of Ethics: Det Etiske Råd, 'Sundhedswearables og big data', 2019 (available here in Danish).

	health data may be processed for the purpose statistic and scientific purposes (og vital societal interest). It is explicitly stressed, that in cases, where health data may be disclosed for criminal investigations based on a court order, this is only allowed in cases concerned with terrorism. In connection with genetic analyses, where test results will be stored in the NGC, patients must on beforehand give a written consent to the analyses, and receive comprehensive information about the storage in the NGC and information regarding the possibility of secondary findings, see section 2.4 in Executive Order no. 359 of 04/04/2019. They should also be informed about the right to opt-out of the further use of data for other purposes, than patient care and related purposes. This gives patients a right to opt out in regard to secondary use of these data for research purposes.

4-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	According to the Health Act (section 41.1, section 42.d and section 43) patient must, as a main rule, consent to the seconday use of data. However, the Health Act also allows for a number of exceptions, such as for planning, management, administration and improvement of health care systems without prior consent from patients. Regarding planning, in Denmark the 5 regions and 98 municipalities have primary responsibility for providing health prevention and health care to the citizens. Section 197 of the Health Act allows the regional and municipality councils to have access to personal health data for planning purposes. With regards to management and administration, according to section 43.2.1 of the Health Act personal health data may be processed, if there is a legal obligation to disclose information to other public authorities and it has a significant impact for the tasks of the authority. In addition, personal health data may be disclosed based on a significant public interest (section 43.2.2) and in cases of audit and control (section 43.2.3). In the context of improvement of health care systems, there are a number of provisions in the Health Act regarding use of health data for quality assurance. Patient data may be processed to assess the qualification of the individual health care professional (section 41.2.6 and section 42d.2), for accreditation, and improvement of quality of health care services (section42d.2-42d.3, section 43.2.4, section 193-193b and section 195-196), and for improvement of patient safety (section 43.2.5 and section 198-202).
Legal basis GDPR	• 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 • Other combination: 6(1)(c) legal obligation + 9(2)(g) substantial public interest on the basis of Union or MS law • Other combination: 6(1)(e) public interest + 9(2)(g) substantial public interest on the basis of Union or MS law
Specific legislation addressing 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.	
National legislation	First it should be noted that when individuals participate in clinical trials (medicines and devices) the informed consent to participation will also include information regarding the obligation to provide access to their medical files and other health information in connection with approval, inspections, control etc. This is in Danish context considered to be primary use of personal data (as opposed to secondary use). The relevant national legislation consists of: • **Medicines Act** (Consolidated Act no. 99 of 16/01/2018) • **Act on Clinical Trials on Medicinal products** (Consolidated Act no. • 1252 of 31/10/2018) • **Act on Medical Devices** (Consolidated Act no. 139 of 15/02/2016) • **Act on Research Ethics Review of Health Research Projects** (Consolidated Act no. 1338 of 01/09/2020) Even though the patient gives consent and is informed about possible future access to medical files etc., the consent of the patient is considered to relate to research participation. There is a separate legal basis for use of patient data for market approval of medicines in the Medicines Act, section 90.2. Consequently in this situation processing personal data for marketing approval is based on a combination of legal obligation based in the Medicines Act and GDPR art. 6(1)(c) and art.9(2)(i) or (h). For medicial devices there does not seem to be a clear legal basis in the Act on Medical Devices and the processing of personal data in this context seems to rely on GDPR art. 6(1)(e) and art.9(2)(i) or (h). In the Act on Research Ethics Review of Health Research Projects it is specifically mentioned in the preparatory work that withdrawal of consent only has effect for future participation, and that both the researchers and authorities will have access to medical files for follow up studies and other purposes. This does not follow as clearly from the other acts (Medicines Act and Act on Medical Devices). There has been some legal discussion about how the use of a GDPR-based consent for the processing of personal data in medical trials could affect the options of future processing of data in situations, where participants withdraw consent to research participation. Due to legal uncertainty, it is recommended not to use a GDPR-based consent for processing of data in clinical trias and other medical trials. Instead GDPR article 9(2)(i) or (h) is considered to provide legal authority to process personal data. Individuals participating in clinical trials should always give consent to the participation. They have the right to withdraw consent for participation in a medical trial, but in this case, the authorities will still be able to access their medical file to comply with the legal obligations laid down in EU and national law to make audits and to investigate adverse events etc. The current legal situation is a bit complex as a new act on Clinical Trials on Medicinal Products was adopted in 2016 to ensure compliance with the new Clinical Trials Regulation (CTR). However, as the CTR has still not come into force, the Danish Act is likewise not operating.
Legal basis GDPR	• 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
Specific legislation addressing 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**	
National legislation	Relevant legislation regarding monitoring is 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).
Legal basis GDPR	• 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
Specific legislation addressing 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**	
National legislation	Section 26 in Consolidated Act no. 1444 of 01/10/2020 on **Measures Against Contagious and other Communicable Diseases** provides the Minster of Health with the authority to issue executive orders regarding mandatory reporting of individual cases of contagious and other communicable diseases. Similarly, section 19 of the **Act regarding Authorisation of Health Care Professionals and Health Care Services** provides a more general legal bases for issuing executive orders regarding health care professionals' notification duties. A number of executive orders have been issued regarding physicians and other health care professionals obligation to notify health care authorities (e.g. the National Board on Health and the Statens Serum Institut in cases regarding contagious and other communicable diseases as well as in regards to other diseases).
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. Section 26 in the Act on Measures Against Contagious and other Communicable Diseases and section 19 in the Act regarding Authorisation of Health Care Professionals and Health Care Services apply, as described above. As an example, section 1 of Executive Order no. 1241 of 26/08/2020 makes it mandatory for laboratories to report cases of COVID-19 directly to Staten Serum Institute (the instiution in charge of dealing with communicable diseases).	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Denmark is complying with EU regulations in the area of food security and notification to the ECDC and other EU warning systems in cases of food born diseases. There is a legal obligation for health care professionals to report cases of a list of specific diseases which may be communicable, which also includes sexually transmitted diseases (executive order no. 277 of 14/04/2000). However, this does not seem to relate specifically to cross-border health threats.
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	For some registers, there are specific provisions in sectoral legislation, others rely on the GDPR and the Danish Data Protection Act. Some are established mostly for research purposes, others primarily for quality assurance purpose, and it may also be serving administrative and planning purposes.
Legal basis GDPR	• 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 • Other combination: 6(1)(c) legal obligation + 9(2)(g) substantial public interest on the basis of Union or MS law
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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 • 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 • Patient organisations • Public sector researchers • Private researchers • Other: access depends on the disease registry, its aim and legal basis.

* Note. 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.

4-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Denmark has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes
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.	Denmark has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Article 9(2)(j) research purposes
National legislation	The legislation differentiates between not for profit researchers and for profit researchers. GDPR article 9(2)(j) and article 89 have been 'activated' in section 10 of the Act no. 502 of 23/05/18 Danish Data Protection Act 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. In situations where data are not processesed for the sole purpose of research, but the processing of data for research will also involve processing of the data for other purposes (e.g. administrative purposes), section 10 does not provide a legal basis, and research must rely on the data subjec's consent. E.g. regulation of clinical trials and trials on medicial devices requires access for authorities to personal data processed during the trial for assessing application of marketing authorisation and to make audits and controls etc. In these situations, data subject's consent is necessesary. In addition, 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).

4-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Denmark the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Denmark:	
Mechanism	• Application to a local research ethics committee • Application to a national research ethics committee • 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)
Application to a local REC or the Danish National Committee on Health Research Ethics is necessary in cases where research subjects (patients or healty research participants) are participating, and also in cases where research is based on tissue samples (without research subjects being involved). In cases where research is performed exclusively on personal data, there is normally no requirement of approval from a regional REC or from the National Committee on Health Research Ethics. However, according to new legislation (Act no. 1436 of 17/12/2019) research projets based on sensitive bioinformatics data and other sensitive data must be approved by a research ethics committee, in cases where there could be a risk of important incidental/secondary findings (such as e.g. projects based on genetic data or advanced imaging).	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
In Denmark, a data altruism system has been created at national level. Sundhed.dk (the national EHR) 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. This is not operating yet. A significant investment also created the NEXT where patients can register if they wish to participate in research. It is a database with patient characteristics that makes them easy to find and enroll into clinical trials. However, it does not involve registration of health data. Through the National Genome Centre, patients who have had genetic sequencing, and where there is no mandatory obligation to store data in the NGC (e.g. because they were sequenced before this regulation came into force) can donate their data to research. When it comes to systems for data altruism, it must also be noted that registry data are available for research with no informed consent, and in this way health data altruism in Denmark could be regarded as mandatory/presumed.	
Legislation has been adopted 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	
There is official support of FAIR and policies to ensure enactment of these principles, but not necessarily in legislation. Both public and private funders increasingly make data sharing mandatory, when privacy concerns or commercial interests do not speak against it. There is an infrastructure for data storage (Danske Data Arkiver) where research data can be stored when a project is finalized. Here one can specify: full open access; access after prior agreement; or no access for other researchers.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research	

purposes
It is easy to have access to data for research purposes, but there is no special system which directly facilitates this. However, the Danish Health Data Authority hosts a number of disease registers and data bases with health related information and facilitates easy access.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Privately funded researchers are not obliged but may choose to do so. Some private research foundations impose a condition of data sharing in their grants. But there is no legislation.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
Denmark has a highly developed ICT infrastructure. It also has multiple systems developed to serve different clinical needs, as well as different types of secondary needs. The main national infrastructural access points are: • Statistics Denmark provides health data combined with other data for research use. Statistics Denmark also hosts StatBank which contains aggregate data that are deemed safe for all citizens to use. • The Serum institute provides registry data (also Statistics Denmark has registry data). • Quality data from the clinic are typically accessed through the quality agency, RKKP. • Genomic data is available through the National Genome Centre • Forskerservice, the research support service provided by the Danish Health Data Authority, provides health data to researchers • KiaP/DAK-E provides general practice data for EHR data for research. General practice data are in repositories administered by the nine commercial system houses (ICT vendors). • Municipalities typically run their own data analytics on data in their own systems, but if they want to compare themselves with other municipalities or research a given topic to set bench marks for their planning they either use the data published by the above institutes. • Patients who self-monitor as part of their treatment and report data to their treating physician can be accessed through the KIH-database and can be linked to data from the national portals through the PIN.

4-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Denmark.

Rights of the patient	How the right can be exercised in Denmark
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Section 36-39 of the Health Act lay down special regulation regarding patients' access to health records and information stored in other documents and registers in the healthcare services. According to section 37, the patient has the right to access patient files and to have access to other data stored in connection with patient care in the healthcare services. Parents can as a main rule access the health record of their child, unless there are special reasons (best interest of the child) to deprive parent's from access. Children at age 15 also have an independent right to access health data, and younger children are also entitled to access based on an assessment of their maturity.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• 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)
In Danish law the right to rectification laid down in GDPR article 16, is – in the public sector – generally interpreted as limited to a right to have a note added which describes the right facts next to the incorrect data. In addition, there is a special regulation in the health care services regarding rectification of data in patient records. See executive order no 530 of 24/05/2000 and section 22 and 24 in the **Act on Authorisation**.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
According to section 24 in the Act on Authorisation it is prohibited to delete data from health records– even if they are clearly incorrect. Instead a note should be added to describe the right facts. See also executive order no 530 of 24/05/2018.	
Article 20 'right to data portability'	• 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)

4-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Denmark to include data from apps and devices in the EHR. In addition, the table displays how Denmark have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
• This is organised nationally. • This is organised regionally. Sundhed.dk gives citizens access to their own records from the secondary sector, including prescriptions, laboratory results, various options for individual choices (organ donation, DNR etc.), and an overview of visits and dates at their GP. Some regional systems, such as the EPIC system, give access to the same information through the platform that supplies data to sundhed.dk. Citizens can also access their electronic correspondence with the GP through the app called Min Læge (which can be downloaded also from sundhed.dk). Patients with chronic illness often self-monitor using webpatient.dk and can see their own data there, or they report using questionnaires developed as Patient Reported Outcomes (PRO). The data then feature on the designated KIH repository, and in some instances patients can access data through the portal (webpatient.dk). There are multiple other apps designed for different needs, and also for different specialities. There is one called Medicinkortet which draws data from the database called The Shared Pharmaceutical Card (Det Fælles Medicinkort), and where citizens can see and renew their prescriptions. For some chronic illnesses they have developed online reporting formats to facilitate telecare and here citizens can usually access data on themselves too.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	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 differs a lot across fields. In some areas wearables are encouraged and some forms of data added, and in others it is not even an option. Some GPs (there are 9 different system houses with different technical specialities) are interested in these data and invite the data, while others reject and do not wish to be responsible for acting on such data. Generally speaking, the data are not seen as particularly relevant when not ordered by the clinician. Typically the algorithms used for generating the data are

	protected by property rights, and it is not possible for the clinician to see how they are construed. Work is underway in the Region of Southern Denmark to establish a curated app-library (as seen in the UK).

Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'

Denmark does not participate in eHDSI.

For years Denmark decided not to be part of BBMRI-ERIC, but this might be changing. Furthermore, Statistics Denmark has been involved in several working groups to facilitate data exchange between different countries.

There are investments through NordForst in better integration of Nordic Registries, but the research that has been funded indicate that it is very difficult to integrate the datasets – not so much for legal reasons, but because all the Nordic countries have PINs for citizens and very data-intensive health infrastructures with old registries, and they thereby have very structured data, but in incompatible coding formats. If they are to integrate the different data it may look almost the same but mean something different. Hence, they have found that combining data sets from different countries can lead to serious mistakes.

Technical standards

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

Policy level	• 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)

Denmark has adopted ISO 27000, but we consider this less related to exchange formats. There are two groups responsible for setting standards for exchange formats, one under MedCom and one coordinated by the Danish Health Data Authority (both groups have reference boards with representatives from the different sectors). It is a precondition for private suppliers that they follow these standards and they have their commercially offered software tested for compatability.

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

There are several national security policy levels, but they work with different aspects of national security. Denmark has adopted ISO 27000. The agency responsible for public e-infrastructures overall security level is the Danish e- Infrastructure Cooperation (DeiC) who also take care of e.g. eduroam connections.

MedCom authenticates access to the Health Data Net (VPN validation). The Agency for Digitization (Digitaliseringsstyrelsen) is involved in some standards for the public security such as the electronic mailbox system (e-Boks), which is also used by the health services for communicating with patients. The Ministry of Defense has developed the Cybersecurity strategy which has designated healthcare as 'critical infrastructure'.

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

Policy level	• There are several national data quality policies which address use of standards for each healthcare provider sector (primary, secondary, tertiary, long term care) • Each region has one data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care) • Each region has several data quality policies which address use of standards for each healthcare provider sectors (primary, secondary, tertiary, long term care)

Each national registry has its own quality specifications and each quality database has it own system (the RKKP, the the Regions Clinical Quality Assurance Program). Quality standards are written into agreements with specialists and GPs. Each subspeciality, such as chronic illness monitoring, has guidelines for each database (KIH-databases).

There used to be an accredition scheme, but it was abolished because it gave extra work, but not ensured better data. There is also the National Indicator Project, National Goals, RKKP, and a system of nurses working with data quality in hospitals each with their own procedures. ISO 27000

described procedures for acting on this too, but it is so generic that in most local environments they are not aware of them, but follow the guidelines developed locally to support data quality.
Agencies which oversee the implementation of technical standards
There are multiple agencies overseeing the implementation of technical standards, which are described above.

4-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	Quality in General Practice (KIAP) https://kiap.dk/
Hospital and medical specialist care	Sundhed.dk www.sundhed.dk
Prescription drugs	Sundhed.dk Overview of Danish Registry Reviews http://www.dsfe.dk/danish-registries/
Self measurements	KIH XDS Repository (KIH) https://www.medcom.dk/systemforvaltning/kih

5 COUNTRY FICHE GERMANY

The following sections provide an overview of the rules for processing of health data currently in place in Germany both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[7]
Note: Germany is a federal state, meaning each state has its own legislation. For the purpose of the survey and this country fiche the federal level has been focused, except in cases where state legislation prevails. The survey also reports on three states in detail: Baden-Württemberg, Bavaria and Berlin, which influences the answers also in the country report. The relationship between state and federal laws was addressed in the survey.

5-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The **Federal Data Protection Act** (BDSG) provides various relevant passages that regulate the way health care providers and professionals process health data for in person care, such as § 22 BDSG on special categories of personal data. In addition, the **German Social Code** (SGB I-XII) regulates the processing of social data (in particular §§ 67 et seq. SGB X) and the **Civil Code** (BGB) covers the treatment contract (§ 630a-§ 630h BGB).
Legal basis GDPR	• Art. 6(1)(a) Consent and Art. 9(2)(a) GDPR Consent • Other combination: Art. 9(2)(h), (3) + Art. 6(1)(b) GDPR as main legal basis (in conjunction with § 22 I Nr. 1 lit. b, II BDSG). • Exceptionally also Art. 9(2)(b) GDPR, § 26 III and IV BDSG, for processing of health data in an employment context
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	§ 22 I b BDSG (NB: state-level provisions, e.g. Hospital laws. NB: restrictions of data processing based on professional secrecy, § 203 Criminal Code (StGB) in combination with § 1 I 2 BDSG).
Legal basis GDPR	• Art. 6(1)(a) Consent and Art. 9(2)(a) GDPR Consent • Art. 9(2)(h) healthcare + Art. 6(1)(b) GDPR contract (treatment contract)
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	• Act for Secure Communication and Applications in the Health Sector, **eHealth Act** [eHealth Gesetz] (21.12.2015) • The **Act on Faster Appointments and Better Care** [Terminservice- und Versorgungsgesetz] (TSVG) (10.05.2019) • The Act to Improve Healthcare Provision through Digitalization and Innovation (**Digital Healthcare Act** – DVG) (18.12.2019) • **Patient Data Protection Act** (PDSG), law governing the protection of electronic patient data in the telematic infrastructure (19.10.2020) • The overwhelming majority of these provisions is implemented in SGB V.

[7] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Germany. The authors of the report take full responsibility for any interpretations in the country fiche.

Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• Art. 6(1)(a) Consent and Art. 9(2)(a) GDPR Consent • Other combination: Art. 9(2)(h), healthcare and Art. 6(1)(b) GDPR, contract (treatment contract).
Specific legislation on **genetic testing**	
National legislation	Germany has specific regulations for genetic testing. The **Genetic Diagnosis Act** (GenDG) applies to genetic testing and analysis for medical purposes and for clarification of parentage as well as in the insurance sector and in working life. It doesn't apply to testing and analysis for research purposes or to testing and analysis based on the Infection Protection Act (IfSG) and related regulations or pursuant to provisions on criminal procedure.

5-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	• § 22 I 1 lit c BDSG describes when personal data may be processed by public and private bodies for reasons of public interest in the area of public health. • The obligation to take measures for quality assurance in the health care sector arises from § 135a II, § 135b II, § 137a III SGB V and § 299 I SGB V. • In accordance with § 136 SGB V *[Guidelines of the G-BA for quality assurance]*, the Joint Federal Committee (Gemeinsamer Bundesausschuss – G-BA) issues guidelines for quality assurance.
Legal basis GDPR	• Art. 6(1)(c) legal obligation + Art. 9(2)(i) GDPR public interest in the area of public health • Other combination: Art. 6(1)(a) consent + Art. 9(2)(a) GDPR consent
Specific legislation addressing 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.	
National legislation	Germany has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	• With regards to **professional law**, the (model) Code of Conduct for physicians working in Germany: obligates the notification of adverse drug reactions in § 6. The Professional Regulation for Pharmacists regulates risk and abuse prevention measures (§ 6 IV). • With regards to **medical devices**, the Medical Devices Act (MPG) § 29 I and II MPG regulate the processing of personal data when reporting risks of medical devices. The Medical Device Safety Plan Ordinance (Medizinprodukte-Sicherheitsplanverordnung - MPSV) regulates the recording, evaluation and prevention of risks associated with medical devices, .e.g. § 3 MPSV sets out reporting obligations and § 11 MPSV sets out the powers of the (competent higher federal) authority. • With regards to **pharmacovigilance**, the pharmacovigilance obligations for the

	marketing authorisation holder are mainly found in the section 10 of the Medicinal Products Act (§ 62 AMG to § 63j AMG). Further pharmacovigilance obligations are defined in § 19 of the Ordinance on the Manufacture of Medicinal Products and Drug Supply (AMWHV). Furthermore the DIMDI-Arzneimittelverordnung (DIMDI-AMV § 1 III 3 DIMDI-AMV is the Ordinance on the database-supported information system on medicinal products of the German Institute for Medical Documentation and Information (DIMDI).
Legal basis GDPR	• Art. 6(1)(c) legal obligation + Art. 9(2)(i) GDPR public interest in the area of public health • Art. 6(1)(c) legal obligation + Art. 9(2)(h) GDPR healthcare • Other combination: Art. 6(1)(a) consent + Art. 9(2)(a) GDPR consent
Specific legislation addressing 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**	
National legislation	• The Act on the Prevention and Control of Infectious Diseases of Humans (IfSG) contains specific legislation at the federal level on infectious diseases. • § 352 SGB V n.V. (*new version*) addresses the processing of data in the electronic patient file by service providers and other persons with authorized access (specifically § 352 No. 16 SGB V n.V. on doctors working for an authority responsible for public health). • § 71 SGB X regulates the transmission for the fulfilment of special legal obligations and powers of notification and § 100 SGB X regulates the duty of the physician or member of another health care profession to provide information.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. In Germany it is regulated by the IfSG (§§ 6, 7, 9, 10 IfSG) that sets out details, e.g. on which diseases must be reported and which pathogens require direct action by the public health department.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Art. 6(1)(c) Legal obligation + Art. 9(2)(i) GDPR public interest in the area of public health • Art. 6(1)(c) legal obligation + Art. 9(2)(h) GDPR healthcare
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	Germany has no general legal provision for creation of disease registries. Some disease registries have a specific legal basis that regulates its creation and operation, while other registries do not have such legal regulation. Examples of some disease registries that do have a specific legal basis are: • Centre for Cancer Registry Data, § 1 Federal Cancer Registry Act (at the Robert Koch Institute (RKI)), Federal Cancer Registry Data Act of August 10, 2009 (BGBl. I p. 2702, 2707), as amended by Article 16a (4) of the Act of April 28, 2020 (BGBl. I p. 960) • Haemophilia Registry, Ordinance on the German Hemophilia Register (Hemophilia Register Ordinance - DHRV), Hemophilia Register Ordinance of May 21, 2019 (Federal Law Gazette I p. 744), as amended by Article 7a of the Act of August 9, 2019 (Federal Law Gazette I p. 1202). • Transplantation Registry, TxRegG, § 15a et seq. Transplantationsregistergesetz (only on federal level), Law on the establishment of a transplant registry of October 11, 2016 (Federal Law Gazette I, p. 2233). • RKI: The other notifiable diseases according to § 6, 7 InfSG are reported to the RKI, where they are registered and statistically processed.
Legal basis GDPR	• Art. 6(1)(c) Legal obligation + Art. 9(2)(i) GDPR public interest in the area of public health • Art. 6(1)(c) legal obligation + Art. 9(2)(h) GDPR healthcare

	• Art. 6(1)(e) public interest + Art. 9(2)(i) GDPR public interest in the field of public health • Other combination: Art. 9 (2)(h) healthcare + Art. 6(1)(b) GDPR contract (treatment contract).
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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

* Note. 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.

5-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Germany has specific legislation on this topic. Legal basis: • Explicit Consent (Art. 9(2)(a) GDPR) – but requiring the data to be de-identified or pseudonymised • Broad consent as defined in national legislation, or in accordance with recital 33 (resolution of the supervisory authorities' conference) • 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. • Art. 9(2)(i) GDPR public interest in the field of public health • Art. 9(2)(j) GDPR research purposes
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	Germany has specific legislation on this topic. Legal basis: • Explicit Consent (Art. 9(2)(a) GDPR) – but requiring the data to be de-identified or pseudonymised

other privately funded research organisations.	• Broad consent (cf. above) • 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. • Art. 9(2)(i) GDPR public interest in the field of public health • Art. 9(2)(j) GDPR research purposes
National legislation	In Germany, the legislation differentiates between not for profit researchers and for profit researchers. SGB V: As regards the Research Data Center, third-party public researchers might have access to the data in the research data center for research purposes, § 303b, e I Nr. 8 and II Nr. 4 SGB V n.V. The access for third-party researches not in the public sector is limited in comparison to the authorized users according to § 303e I SGB V n.V. and depends on the approval by the research data center according to § 303e V 1 No. 2 SGB V n.V.

5-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Germany the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Germany:	
Mechanism	• The data controller provides direct access upon proof of agreement of a research ethics committee or DPA • Application to a centralised data governance and access body (hence other than each data controller / data custodian individually) • Other: provisions for health insurance providers.
§ 363 SGB V n.V. "Processing of data of the ePA for research purposes" sets out that data processors of the *elektronische Patientenakte* (ePA, the German EHR managed by the patient), may transmit pseudonymised and encrypted data for research purposes to the Research Data Center with informed consent of the patient. § 303e SGB V n.V. stipulates which authorized users can access this data held in the Research Data Center and for which research purposes. § 287 SGB V n.V. Research projects: defines provisions that relate to social data held by the health insurance providers and personal data use at the Associations of Statutory Health Insurance Physicians. The health insurance funds and providers are also permitted to use the anonymised or pseudonymized stock of data collected within the framework of §§ 303a et seq. SGB V including for research purposes in order to fulfil their tasks (§ 303e I Nos. 3, 4 SGB V). § 75 SGB X defines the provisions for the transmission of social data for research and planning.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
In Germany, a data altruism system has been created at national level. § 363 SGB V n.V. Processing of data of the ePA for research purposes states that (1) 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, which are: improving the quality of care; research, in particular for longitudinal analyses over longer periods of time, analyses of treatment processes or analyses of the care provision; support of political decision-making processes for the further development of statutory health insurance; and performing health reporting tasks. (4) The data released to the Research Data Center may be processed by the Research Data Center for the fulfilment of its tasks and, upon request, may be made available to the authorized users pursuant to § 303e I Nos. 6, 7, 8, 10, 13, 14, 15 and 16 SGB V, e.g. health care research and health reporting institutions, universities and university hospitals, institutions engaged in independent scientific research and several national institutes of the healthcare sector for the	

fulfilment of their own tasks.

(8) Notwithstanding the data release to the research data center as provided for in the above paragraphs, 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.

Legislation has been adopted 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

Germany has specific legislation on this topic. The most relevant provisions of the telematics infrastructure are:

- § 306 SGB V n.V. (Telematics infrastructure: The telematics infrastructure is the interoperable and compatible information, communication and security infrastructure which serves to network service providers, payers, insured persons and other players in the health care system as well as rehabilitation and care.)
- § 311 V SGB V n.V. (Tasks of the Gesellschaft für Telematik (GfT))
- § 325 III SGB V n.V. (Approval of components and services of the telematics infrastructure)
- § 342 SGB V n.V. (Offer and use of the ePA)
- § 360 V SGB V n.V. (Transmission of prescriptions by SHI-accredited doctors in electronic form) requires that the functionality and interoperability of the components must also be ensured in the case of in-house developments by the Gesellschaft für Telematik.
- The fourth subtitle of the Patient Data Protection Act contains the provisions covering the specifications for technical requirements and the semantic and syntactic interoperability of data such as § 354 SGB V n.V. and § 355 SGB V n.V.
- § 355 VI and VII SGB V n.V. provide medical terminology that ensures this semantic interoperability for medical data in the ePA
- § 375 SGB V n.V. (Creation of statutory ordinance in form of more detailed guidelines for the specification of open and standardized interfaces for information technology systems)
- The whole twelfth subtitle (§§ 384-393 SGB V n.V.) examines the interoperability directory and defines detailed regulations.
- For data sent to the Research Data Center, specific measures related to the infrastructure are included in §§ 303a et seq. SGB V n.V.

A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes

Germany has adopted a system to facilitate this.

§ 363 SGB V n.V. Processing of data of the ePA for research purposes states that

(1) 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 n.V.

Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**

- Germany has not adopted specific legislation.

Data access infrastructure 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
- There are several sector specific national systems to share data for secondary use.

Next to the Research Data Center, two other infrastructures exist/are being built in Germany.

A new infrastructure is the national research data infrastructure (NFDI). It aims to systematically manage scientific and research data, provide long-term data storage, backup and accessibility, and network the data both nationally and internationally. The NFDI will bring multiple stakeholders together in a coordinated network of consortia tasked with providing science-driven data services to research communities. The first consortia have taken up work in October 2020.

The Medical Informatics Initiative (MII) consists of university hospitals and partners and aims to create – besides technical harmonization – an organizationally uniform and legally secure framework that enables the provision and use of patient data and biomaterials as well as the use of analysis methods and routines for medical research.

5-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Germany.

Rights of the patient	How the right can be exercised in Germany
Article 15 'right to access data concerning him or her'	• 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: See word document for this answer.
Relevant legislation on Article 15 GDPR in Germany is provided in (but not limited to) • § 34 BDSG 'Right of access by the data subject', which provides derogations to Art. 15 GDPR. • § 83 SGB X 'Right of data subjects to information', applicable to social data. • § 341 SGB V n.V. The ePA sets out the new electronic record kept by the insured person. It is intended to provide the insured persons, upon request, with barrier-free electronic information, in particular on findings, diagnoses, implemented and planned therapy measures and treatment reports, for cross-institutional, cross-disciplinary and cross-sectoral use for health care purposes, in particular for the targeted support of anamnesis and diagnosis. • In addition, § 308 SGB V, §§ 336, 337, 334 SGB V n.V. apply to the rights of the (insured) patient.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a formal national 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) GDPR
Relevant legislation on Article 16 in Germany is provided in (but not limited to) • § 28 III BDSG provides derogations to Art. 16 GDPR when data is processed for archiving purposes in the public interest. • § 84 SGB X 'Right of rectification, erasure, restriction of processing and opposition', applicable to social data. • § 291c SGB V n.V. on the withdrawal, blocking or further use of the electronic health insurance card after change of health insurance provider; and exchange of the electronic health insurance card.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions
Relevant legislation on Article 17 in Germany is provided in (but not limited to) • § 35 BDSG: Right to erasure provides derogations to Art. 17 GDPR. • § 84 SGB V: Right of rectification, erasure, restriction of processing and opposition, applicable to social data • § 337 SGB V n.V. Right of the insured persons to process data and to grant access rights to data, according to § 337 II SGB V n.V. The insured person is entitled to independently delete data in an application. • For the medical records kept by the doctor: § 630f BGB: Right to erasure the documentation of the treatment after ten years.	
Article 20 'right to data portability'	• through a formal national 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

5-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Germany to include data from apps and devices in the EHR. In addition, the table displays how Germany have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
• This is organised nationally. • This is organised by individual health services. The new Patient Data Protection Act implements a new electronic health record, § 341 SGB V n.V.. This is intended to allow patients to control who is able to see their data and know what data specifically is being held (§ 352 SGB V n.V.), and enable them to request deletion of data from the electronic patient file (§ 344 III SGB V n.V.) or to add data to it (§§ 347 SGB V n.V. et seq.). Physician-controlled data systems are regulated by §§ 630a et seq. BGB, § 630g BGB and § 630f III BGB. According to § 630f I BGB, for the purpose of documentation, the treating physician is obliged to keep a patient file in paper or electronic form during or soon after the treatment. According to § 630g BGB (1) the patient permitted to inspect the complete medical records concerning him/her and (2) can also request electronic duplicates of the medical records.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• Healthcare professionals are allowed to incorporate patient generated data into healthcare professional/ provider held EHRs.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Germany does not yet participate in eHDSI but plans to do so by 2025. § 219c SGB V establishes the National Contact Point. § 311 III SGB V n.V. Tasks of the Gesellschaft für Telematik, regulates that the GfT performs tasks at the European level, in particular in connection with the cross-border exchange of health data.	
Technical standards	
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	
Policy level	• 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)
The basis for the answer above is the Patient Data Protection Act. The most relevant provisions of the telematics infrastructure that have been adopted as part of the new Patient Data Protection Act are: • § 306 SGB V n.V. (Telematics infrastructure) • § 311 V SGB V n.V. (Tasks of the Gesellschaft für Telematik) • § 325 III SGB V n.V. (Approval of components and services of the telematics infrastructure) • § 342 SGB V n.V. (Offer and use of the ePA) • § 360 V SGB V n.V. (Transmission of prescriptions by SHI-accredited doctors in electronic form) • The fourth subtitle of the Patient Data Protection Act contains the provisions covering the specifications for technical requirements and the semantic and syntactic interoperability of data, such as: § 354 and § 355 SGB V n.V. • § 355 VI and VII SGB V n.V. (Medical terminology ensuring semantic interoperability) • § 375 SGB V n.V. Creation of statutory ordinance (more detailed guidelines for the specification of open and standardized interfaces for information technology systems) • The whole twelfth subtitle of the Patient Data Protection Act (§§ 384-393 SGB V n.V.) examines	

the interoperability directory and defines detailed regulations.
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely
Policy level: • There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care) • Each region has several data security policies which address use of security standards in each healthcare provider sectors (primary, secondary, tertiary, long term care)
The most relevant provisions are provided in: • § 311 II, VI SGB V n.V. (Tasks of the Gesellschaft für Telematik) • § 315 I, II SGB V n.V. (Binding nature of the resolutions of the Gesellschaft für Telematik) • § 311 I, VI SGB V n.V. (Tasks of the Gesellschaft für Telematik) • § 324 I-III SGB V n.V. (Approval of providers of operating services) • § 325 I-III, V SGB V n.V. (Approval of telematics infrastructure components and services) • § 327 I, II, IV SGB V n.V. (Other telematics infrastructure applications; confirmation procedures) • § 329 I SGB V n.V. (Measures to avert threats to the functioning and security of the telematics infrastructure) • § 331 I, II SGB V n.V. (Measures for monitoring operations to ensure the security, availability and usability of the telematics infrastructure) • § 333 I-III SGB V n.V. (Review by the Federal Office for Information Security) • § 339 I-IV SGB V n.V. (Avoidance of disruptions in the information technology systems, components and processes of the telematics infrastructure) • § 360 V SGB V n.V. (Transmission of prescriptions by SHI-accredited doctors in electronic form) • § 388 I-III SGB V n.V. (Recommendation of standards, profiles and guidelines of information technology systems in health care as a reference)
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
Policy level: • There are several national data quality policies which address use of standards for each healthcare provider sector (primary, secondary, tertiary, long term care)
Data quality policies are to emerge in the context of the telematics infrastructure as designed by the GfT, BSI and the BMG. Certainly, the most remarkable progress can be observed within the context of interoperability. Additionally, the MII initiative has addressed data quality issues. Regarding research it is worth noting that one of the tasks of the Research Data Center is to perform quality assurance of data (§ 303d I No. 2 SGB V Research Data Center).
Agencies which oversee the implementation of technical standards
The Gesellschaft für Telematik is the main agency to oversee the implementation of technical standards, supported by other agencies in Germany.

5-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	https://www.krebsregister-bw.de/patienten-interessierte
Hospital and medical specialist care	https://www.medizininformatik-initiative.de/de/CORD
Prescription drugs	https://www.abda.de/ueber-uns/die-abda/
Self measurements	https://www.dkgev.de/service/

6 COUNTRY FICHE ESTONIA

The following sections provide an overview of the rules for processing of health data currently in place in Estonia both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[8]

6-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	This is regulated in the Health Services Organisation Act in clause 4^1 (https://www.riigiteataja.ee/en/eli/518052020003/#para4b1) Health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data required for the provision of a health service, including personal data of special categories, without the permission of the data subject. Please see the chapter 1, general provisions.
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(h) provision of health or social care
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	This is regulated in the Health Services Organisation Act in clause 4^1(1) (https://www.riigiteataja.ee/en/eli/518052020003/#para4b1) Health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data required for the provision of a health service, including personal data of special categories, without the permission of the data subject. This is the main legal basis. This allows healthcare providers and healthcare professionals to share health data among themselves for healthcare provision purposes. In Estonia, there is also a national Health Information System. This is regulated in the Health Services Organisation Act, in clause 59^1(1) (https://www.riigiteataja.ee/en/eli/518052020003/#para59b1) The Health Information System processes the data related to the area of health care for entry into and performance of contracts for the provision of health services, for ensuring the quality of health services and the rights of patients and for the protection of public health, including for maintaining registers concerning the state of health, for the organisation of health statistics and for the management of health care. The controller of the Health Information System is the Ministry of Social Affairs. Please see the chapter 5^1, Health Information System.
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	

[8] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Estonia. The authors of the report take full responsibility for any interpretations in the country fiche.

National legislation	This is regulated in the following Acts: • Health Services Organisation Act, clause 50^3(3): https://www.riigiteataja.ee/en/eli/518052020003/#para50b3 In case of cross-border health services, the Member State providing treatment shall be the Member State of the European Union in whose territory health services are provided to a patient. In case of telemedicine it shall be deemed that health services are provided in the Member State in which the health care provider has been established. • Health Information System regulation of the Government of the Republic: https://www.riigiteataja.ee/akt/126022020002 (Not available in English). • Medical Devices Act: https://www.riigiteataja.ee/en/eli/528052020007/
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(h) health or social care
Specific legislation on **genetic testing**	
National legislation	Estonia does not have specific regulations for genetic testing. Accreditation in Estonia is voluntary, but many laboratories are accredited, including Tartu University Hospitals, and also for genetic testing.

6-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	This is regulated in the following Acts: Health Services Organisation Act, clause $4^1(1^1)2$) (https://www.riigiteataja.ee/en/eli/518052020003/#para4b1) Health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data, including personal data of special categories with the aim and to the extent specified in clause 56(1)7) of this Act. (https://www.riigiteataja.ee/en/eli/518052020003/#para56) In addition to legislation specified in this Act, the Minister responsible for the area shall establish the quality assurance requirements for health services. This is regulated in the Quality assurance requirements for health services (https://www.riigiteataja.ee/akt/115012019005; Available only in Estonian). Public Health Act, clause 1(1) (https://www.riigiteataja.ee/en/eli/529082019007/#para1). The purpose of this Act is to protect human health, prevent diseases and promote health, which is to be achieved through the performance of duties by the state, local governments, legal persons in public law, legal persons in private law and natural persons, and through the system of national and local measures. In clause 8(1)12) of the same Act, (https://www.riigiteataja.ee/en/eli/529082019007/#para8), the duties of the Ministry of Social Affairs are described: To collect information on the health of the population,

	and process personal data for the development and implementation of national health and health care policies in accordance with the Personal Data Protection Act and Public Information Act.
Legal basis GDPR	• 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
Specific legislation addressing 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.	
National legislation	Patient consent.
Legal basis GDPR	Other: 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation addressing 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**	
National legislation	This is regulated in the following Acts: Medical Devices Act (https://www.riigiteataja.ee/en/eli/528052020007/): Clause 1(1) (https://www.riigiteataja.ee/en/eli/528052020007/#para1) With the aim of protecting the safety and health of persons, this Act provides the requirements for: 1) medical devices and accessories (hereinafter medical devices) and the manufacture thereof; 2) placing on the market and putting into service of medical devices; 3) providing clinical evaluation of medical devices; 4) the professional users of medical devices. 5) the sale of medical devices on the basis of medical device card. Clause 27(7) (https://www.riigiteataja.ee/en/eli/528052020007/#para27) The persons providing information on an adverse incident shall guarantee the protection of the personal information of a patient or lay user and the business secrets of an undertaking which become known to them in the course of processing the adverse incident. Medicinal Products Act (https://www.riigiteataja.ee/en/eli/518052020005/), Clause 1(1)https://www.riigiteataja.ee/en/eli/518052020005/#para1 This Act regulates the handling of medicinal products, issue of medical prescriptions, granting of marketing authorizations, clinical trials and advertising of medicinal products, and supervision over and responsibility in the field of medicinal products for the purpose of ensuring the safety, quality and efficacy of medicinal products used in Estonia and promoting the use of medicinal products for their intended purposes.
Legal basis GDPR	• 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
Specific legislation addressing 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**	
National legislation	This is regulated in the Communicable Diseases Prevention and Control Act (https://www.riigiteataja.ee/en/eli/518052020002/) Clause 1(1) (https://www.riigiteataja.ee/en/eli/518052020002/#para1) This Act regulates the way in which the control of communicable diseases is organised and the procedure for the provision of health care services to infected persons (hereinafter provision of medical care), and sets out the obligations of the state, local governments, legal persons and natural persons in the prevention and control of communicable diseases. Clause 19(5) (https://www.riigiteataja.ee/en/eli/518052020002/#para19). The information specified in subsections (2) and (4) of this section shall be communicated together with the personal data of a data subject.

	Clause 21(6[1]) (https://www.riigiteataja.ee/en/eli/518052020002/#para21). Data on suspicion or diagnosis of a communicable disease shall be communicated together with the personal data of a data subject, if necessary. The list of communicable diseases which require the communication of data together with the personal data of a data subject shall be established by a regulation of the minister responsible for the area.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. The legislation that allows for such direct reporting is the Communicable Diseases Prevention and Control Act, clause 19(2) (https://www.riigiteataja.ee/en/eli/518052020002/#para19). Physicians are required to inform the local agency of the Health Board immediately of any suspicion of an extremely dangerous communicable disease.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 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
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	There is a specific regulation for each registry. See Public Health Act, Chapter 2 Databases (https://www.riigiteataja.ee/en/eli/529082019007/consolide#para14b1)
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • A patient may be given access to any data concerning themselves • 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 • Public sector researchers • Private researchers • Other: There is a specific regulation for each registry.

* Note. 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.

6-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Estonia has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised • 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
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.	Estonia has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Explicit Consent (Article 9(2)(a)) – but requiring the data to be de-identified or pseudonymised • 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)(j) research purposes
National legislation	In Estonia, the legislation does not differentiate between not for profit researchers and for profit researchers. The relevant legislation concerns the following: Personal Data Protection Act6(1)-(6) (https://www.riigiteataja.ee/en/eli/523012019001/#para6) Public Health Act clause 8(1)8) (https://www.riigiteataja.ee/en/eli/529082019007/#para8). The duties of the Ministry of Social Affairs are to co-ordinate research relating to health protection, disease prevention and health promotion. Public Health Act clause 8(1)12) (https://www.riigiteataja.ee/en/eli/529082019007/#para8). The duties of the Ministry of Social Affairs are to collect information on the health of the population, and process personal data for the development and implementation of national health and health care policies in accordance with the Personal Data Protection Act and Public Information Act.

6-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Estonia the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Estonia:	
Mechanism	• Application to a local research ethics committee • Application to a national research ethics committee • The data controller provides direct access upon proof of agreement of a research ethics committee or DPA
The relevant regulation is the Personal Data Protection Act, clause 6(1)-(6) (https://www.riigiteataja.ee/en/eli/523012019001/#para6)	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Estonia did not adopt such a system.	
Legislation has been adopted 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	
Estonia has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research	

purposes
Estonia has adopted a system to facilitate this. This is regulated in the general regulation of the National Health Information System.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Privately funded researchers are not obliged but may choose to do so.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
There are several national systems to share data for secondary use. Depending on the type of database, different regulations apply: The Health Information System is regulated according to Health Services Organisation Act, state databases according to the Public Health Act. Health Services Organisation Act (https://www.riigiteataja.ee/en/eli/518052020003/). Relevant sections are: Chapter 5^1 (https://www.riigiteataja.ee/en/eli/518052020003/#para59b1) Clause 59^1(1) (https://www.riigiteataja.ee/en/eli/518052020003/#para59b1). The Health Information System processes the data related to the area of health care for entry into and performance of contracts for the provision of health services, for ensuring the quality of health services and the rights of patients and for the protection of public health, including for maintaining registers concerning the state of health, for the organisation of health statistics and for the management of health care. Clause 59^3(7) (https://www.riigiteataja.ee/en/eli/518052020003/#para59b3). In addition to the provisions of subsection (6) of this section, personal data shall only be issued with the consent of the data subject, and for the purposes of scientific or historical research and national statistics or for establishing the truth in offence or judicial proceedings without the consent of the data subject. Clause 59^4(1) (https://www.riigiteataja.ee/en/eli/518052020003/#para59b4). The Research Ethics Committee evaluates the need to issue personal data from the Health Information System for the purposes of scientific research and statistics and the justification thereof. Public Health Act (https://www.riigiteataja.ee/en/eli/529082019007/). Relevant sections are: Chapter 2^1 (https://www.riigiteataja.ee/en/eli/529082019007/#para14b1) Clause 14^1(2) (https://www.riigiteataja.ee/en/eli/529082019007/#para14b1). The data of the database or information system specified in §§ 14^2–14^5 and 14^7 of this Act shall be issued in a non-personalised form. Personalised data shall be issued with the consent of the data subject or for scientific and historical research, statistics or establishing the truth in criminal proceedings.

6-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Estonia.

Rights of the patient	How the right can be exercised in Estonia
Article 15 'right to access data concerning him or her'	• Through a formal national 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: Via the National Health Information System patient portal. Patients can access their health data, that has been made available to them. They have to identify themselves with eID.

Relevant legislation: Law of Obligations Act, clause 769 (https://www.riigiteataja.ee/en/eli/515012020004/#para769). A provider of health care services shall document the provision of health care services to each patient pursuant to the requirements and shall preserve the corresponding documents. The patient has the right to examine these documents and to obtain copies thereof at his or her own expense, unless otherwise provided by law.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
Relevant regulation: Health Services Organisation Act (https://www.riigiteataja.ee/en/eli/518052020003/), clause 59^3(3) (https://www.riigiteataja.ee/en/eli/518052020003/#para59b3). A patient has the right to prohibit the access of persons specified in subsections (2) and (2^1) of this section to the personal data in the Health Information System. That applies only to the national Health Information System, not to the healthcare providers ones. To prohibit the access does not mean to erase.	
Article 20 'right to data portability'	• Through a formal national 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
The health data processing in Estonia is based on Health Services Organisation Act 4^1(1) (https://www.riigiteataja.ee/en/eli/518052020003/#para4b1). Health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data required for the provision of a health service, including personal data of special categories, without the permission of the data subject. The right to health data is based on EU 2016/679 and Law of Obligations Act, clause 769 (https://www.riigiteataja.ee/en/eli/515012020004/#para769) A provider of health care services shall document the provision of health care services to each patient pursuant to the requirements and shall preserve the corresponding documents. The patient has the right to examine these documents and to obtain copies thereof at his or her own expense, unless otherwise provided by law	

6-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Estonia to include data from apps and devices in the EHR. In addition, the table displays how Estonia have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
• This is organised nationally. Relevant legislation: Health Information System Health Services Organisation Act, Chapter 5^1 (https://www.riigiteataja.ee/en/eli/518052020003/#para59b1)	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• Healthcare professionals are allowed to incorporate patient generated data into healthcare professional/ provider held EHRs.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	

Estonia participates in eHDSI through sharing summary records and prescriptions.
Technical standards
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
Policy level • 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)
Estonia uses the following technical standards: • ICD-10 https://www.who.int/classifications/icd/en/ • HL7 http://www.hl7.org/ • LOINC https://loinc.org/ • DICOM https://www.dicomstandard.org/
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely
Policy level • There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
The following technical standards are addressed in policies in Estonia: Three-level IT baseline security system (ISKE) (https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html https://www.ria.ee/sites/default/files/content-editors/ISKE/regulation-the-system-of- security-measures-for-information-systems-2007-12-20.pdf). ISKE is Estonian's own information security standard for public sector. ISKE is based on a German information security standard (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html). Additionally, other information security standards are allowed (ISO, ITIL, NIST).
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
Policy level • There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
The quality assurance requirements for health services can be found here: https://www.riigiteataja.ee/akt/115012019005. Available only in Estonian.
Agencies which oversee the implementation of technical standards
Ministry of Social Affair (https://www.sm.ee/en) Health and Welfare Information Systems Centre (https://tehik.ee/) National Institute for Health Development (https://tai.ee/en/) Information System Authority (https://www.ria.ee/en)

6-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	East-Tallinn Central Hospital, research department, https://www.itk.ee/en Tartu University Hospital, Estonian Myocardial Infarction Register, http://www.infarkt.ee/en

7 COUNTRY FICHE IRELAND

The following sections provide an overview of the rules for processing of health data currently in place in Ireland both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[9]

7-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	Common Law: there is a common law duty of confidentiality imposed on healthcare providers with regard to information confided in them by the patient. The torts relevant to privacy are trespass, nuisance, and the equitable action for breach of confidence. Each tort supports the components of personal privacy. The Constitution: Privacy is a personal right derived from Article 40.3 of the Constitution. It is an unenumerated right or an unwritten right: -1 ◦ The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen. Professional Codes: Irish medical professional codes impose a strict the duty of confidentiality on practitioners. A breach of this duty is serious and exposes practitioners to a wide range of potential professional sanctions. Legislation and national law governing processing of health data for the provision of healthcare: • GDPR; • Data Protection Act 2018 - Sections 52and 53 give effect to Article 9(2)(h) and (i) of the GDPR respectively; they permit processing of personal data for health-related purposes and public interest in the area of public health; • Health Acts 1947- 2020-obligation to provide healthcare ; • Disability Act 2005- section 12 -exchange of information between service provider and healthcare professionals- based on consent; • Mental Health Act 2001; • Medical Practitioners Act 2007; • Common Law and Constitutional Law.
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	No specific legislation has been adopted on this topic. However, wider legislation is in place which addresses certain aspects of such data sharing. They include: • Necessity – disclosures to members of the health care team and support staff are often necessary for safe, efficient and effective care, such disclosures must

[9] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Ireland. The authors of the report take full responsibility for any interpretations in the country fiche.

	make clear the information is confidential • Patients' rights: patients must be informed and may object to such disclosures. Such objection must be respected but may result in medical transfer not being made. Guidance for professionals is set out in 'The Irish Medical Council – Guide to Professional Conduct and Ethics for Registered Medical Practitioners' which is grounded in the Medical Practitioners Act 2007. Legislation and National Law: • GDPR, • Data Protection Act 2018 - Sections, 52 and 53 give effect to Article 9(2)(h) and (i) of the GDPR respectively; they permit processing of personal data for health-related purposes and for public interest in the area of public health; • Health Acts 1947- 2020-obligation to provide healthcare; • Medical Practitioners Act 2007; • Nursing and Midwifery Act 2011, Mental Health Act 2001; • Disability Act 2005- section 12 - exchange of information between service provider and healthcare professionals- based on consent; • Common Law and Constitutional Law.
Legal basis GDPR	• 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 While the Data Protection Act 2018 does not lay down 6(1) (c), such legal obligation are provided for in a wide array of Acts, SIs, Common Law and Constitutional obligations thus fufilling the requirements of GDPR.
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	The Data Protection Act 2018.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	There is no prescriptive lawful basis and determining the lawful basis depends very much on the circumstances and purpose i.e. it is a public, private health entity or national health authority. Consent can be used but is not recommended. The follwoing would be the most commonly used lawful basis in this scenario: • 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)(f) legitimate interest + 9(2)(h) health or social care While the Data Protection Act 2018 does not lay down 6(1) (c), such legal obligation are provided for in a wide array of Acts, SIs, Common Law and Constitutional obligations thus fulfilling the requirements of GDPR.
Specific legislation on **genetic testing**	
National legislation	Ireland has specific regulations for genetic testing. Disability Act 2005, Part 4 Sections 41-45 – provides safeguards for the use of information obtained from genetic testing. The provisions aim to ensure that people who may be affected by genetic disorders will not be subject to any unreasonable requirements from an employer or an insurance or mortgage provider.

7-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	GDPR. Section 52(e) of the Data Protection Act 2018 - permits processing of special categories of personal data for the management of health or social care systems. Sections 53 gives effect to Article 9(2)(i) of the GDPR permitting the processing of personal data for public interest purposes and Section 43 allows for processing of special categories of data for statistical purposes Article 9(2)(j). The Health (Provision of Information Act) 1997 legislates the the provision of information to the National Cancer Registry Board, the Minister for Health and certain other health bodies, for the purposes of the provision of cancer screening programmes, and to provide for related matters ; The Statistics Act 1993 provides the legislative basis for the compilation and dissemination of offical statistics. It provides the statutory basis for the collection and use of specific information, including personal health information. This allows for the collection of health and social information in order to generate statastics on acute hospital services, on disability , carerers and voluntary activities.
Legal basis GDPR	• 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)(e) public interest + 9(2)(i) public interest in the field of public health • 6(1)(f) legitimate interest + 9(2)(h) healthcare While the Data Protection Act 2018 does not lay down 6(1) (c), such legal obligation are provided for in a wide array of Acts, SIs, Common Law and Constitutional obligations thus fulfilling the requirements of GDPR
Specific legislation addressing 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.	
National legislation	The Health Products Regulatory Authority (HPRA) operates the national system for recording and reporting details of suspected issues occurring in Ireland which are notified in association with the use of medicines. These reports are submitted to the HPRA directly by healthcare professionals and patients.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	The HPRA operates the national system for recording and reporting details of suspected adverse reactions occurring in Ireland which are notified in association with the use of medicines. These reports are submitted to the HPRA directly by healthcare professionals and patients. They are also submitted indirectly from pharmaceutical companies, through the European Medicines Agency's database, known as 'EudraVigilance'.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	Infectious Diseases Regulations 1981 Data Protection Act 2018 Section 53 Decision 1082/2013/EU the Health Protection Surveillance Centre (HPSC) is required to

	report information on specified infectious diseases to the European Centre for Disease Prevention and Control (ECDC). HPSC is also required to report at European Level – to ECDC, other member states and the European Commission) in the event of outbreaks of infectious diseases extending to, or at risk of extending to, other MS. In general, such reporting does not include personally identifiable information.
Under MS legislation, 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, it is possible. Infectious Diseases Regulations 1981- the collection of surveillance data is standardised on a national basis. All medical practitioners, including clinical directors of diagnostic laboratories, are required to notify the Medical Officer of Health (MoH) of notifiable diseases. Laboratory notifications are made electronically through the Computerised Infectious Disease Reporting System (CIDR).	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	There is legislation only for one disease registry: the National Cancer Registry. It is legislated by the Health (Provision of Information) Act 1997.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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 • 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 • Public sector researchers • Private researchers • Private sector organisations

* Note. 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.

7-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Ireland has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes

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.	Ireland has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Article 9(2)(j) research purposes
National legislation	The specific legislation for both researchers in the public sector and not in the public sector are the Data Protection Act 2018 Section 42 & 54 and The Health Research Regulations (HRRs) 2018. The Health Research Regulations 2018 came into force in August 2018 establishing a number of conditions regarding governance processing & procedure of personal data for health research purpose. Of these conditions "explicit consent", has emerged as a particular challenge for Irish researchers. The GDPR grants a scientific research an exemption9(2)(j) but the HRRs apply a mandatory "explicit consent" requirement as a safeguard of processing. The HRRs permit the use of personal data for health research purposes without "explicit consent" in exceptional circumstances. To avail of this concession researchers must submit an application to the national Health Research Consent Declaration Committee, established by the HRRs, for a consent declaration, demonstrating that substantial public interest exists and that "explicit consent" is not feasible.

7-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Ireland the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Ireland:	
Mechanism	• Application to a local research ethics committee • Application to a national research ethics committee
Health Research Regulations 2018 – Section 3 (1)(b)(i)- An application and approval from a Research Ethics Committee is always necessary before research can be commenced.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Ireland did not adopt such a system.	
Legislation has been adopted 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	
Ireland has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Ireland did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Ireland has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
When a researcher wishes to access data held in EHRs for secondary use, an application to the data controller - healthcare provider or healthcare professional is necessary.	

7-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Ireland.

Rights of the patient	How the right can be exercised in Ireland
Article 15 'right to access data concerning him or her'	• Through an access request to the data controller.
Article 61 of the Data Protection Act 2018.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a rectification request to the data controller
Article 61 of the Data Protection Act 2018.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, although with some restrictions.
Article 61 of the Data Protection Act 2018.	
Article 20 'right to data portability'	• A patient needs to make a request to the data controller.

7-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Ireland to include data from apps and devices in the EHR. In addition, the table displays how Ireland have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Ireland does not yet participate in eHDSI but plans to do so by 2025.	
Technical standards	
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	
Policy level	• 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) • No, there are no national or regional policies to ensure use of standards for data interoperability
Ireland has no one standard to drive the interoperability of health records. Institutions have used various methods of transferring data from one institution to another including HL7, however, given the varying technologies used in each institution there is currently nothing driving this.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care) • No, there are no national or regional data security policies to ensure use of standards for data security
In 2019 the Department of Communications, Climate Action & Environment published New Cyber Security Guidelines for Operators of Essential Services. Health sector is considered an OES. The sector must be in line with NIST Guidelines and Controls. There are over 100 expected controls, across the 5 NIST areas are included (Identify, Protect, Detect, Respond, Recover).	
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	
Policy level	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.
Agencies which oversee the implementation of technical standards	
The Department of Communications, Climate Action & Environment published New Cyber Security Guidelines for Operators of Essential Services	

8 COUNTRY FICHE GREECE

The following sections provide an overview of the rules for processing of health data currently in place in Greece both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[10]

8-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	**Law 3418/2005** (Code of Medical Ethics), Article 14, as it has been codified by the presidential decree 28/2015 on the access to public documents provides for the obligation of doctors to keep medical files in electronic form (or non-electronic). Clinics and hospitals are also obliged to keep files and results of all clinic and paraclinical examinations. This provision also describes the content of medical files and provides that patients' data, collected by private clinics and primary health care, must be stored for ten years, since the last visit of the patient and in any other case for twenty years. The law prohibits access of third persons to patients' medical files, with the exception of judicial authorities, state authorities having right to access and any third person invoking a legal interest. **Law 4600/2019**, Article 83(1) states that by decision of the Minister of Health, National Patient Registries can be established and operate on the basis of specific criteria each time, such as the use of treatment in which the cost/the morbidity/the mortality is increased, the high incidence of diseases in the general population, the use of specific treatment, the recording of rare diseases, the purposes of pharmacovigilance. The establishment and operation of the above 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. The establishment and operation of these Registries shall be carried out, in accordance with international scientific standards and in particular with EU law and specific national regulations, relevant guidelines and recommendations of the WHO and the European Center for Disease Prevention and Control (ECDC). Law 4600/2019, Article 84(4)(2) states that the Individual Electronic Health Record contains the individual health history of the recipient of health services, as well as data, assessments and information of all kinds about the condition and clinical development of this person, as a patient, throughout the treatment process. The content of the Individual Electronic Health Record is maintained for life and is undivided and mandatory at national level. Law 4600/2019, Article 84(4)(5) states that any natural or legal person lawfully keeps or processes an individual file or Patients Registry, including registries or individual files of insured persons of the EOPYY (National Organization for the Provision of Healthcare Services) or Social Security Institutions, must register in the Individual

[10] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Greece. The authors of the report take full responsibility for any interpretations in the country fiche.

	Electronic Health Record any patient-related health data. **Joint Ministerial Decision 2650/2020** regulates more specific technical issues for the operation of the National Patient for COVID-19, in accordance with the provisions of the article 29 of the Legislative Act published on 30.3.2020 "Measures to deal with the pandemic of Covid-19 and other urgent provisions" and article 83 of L. 4600/2019. **Law 4722/2020**, Article 12 par. 1 and 2 state that the National Organization of Public Health (EODY) has access to all the information of the COVID-19 Patient Registry and to the searching possibilities within the relevant platform in the context of the epidemiological investigation carried out by the Directorate of Epidemiological Surveillance and Intervention for Patients. EODY also has access to data from hospitals, primary health care facilities, laboratories, the Health Operations Center of the National Emergency Center and the General Secretariat for Civil Protection, with the aim of completing the Register and implementing corrections in the sections of the platform, such as the section of residence and the laboratory test's result. The above law is applied in accordance with GDPR 679/2016 and Law 4624/2019.
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Law 4600/2019, Article 84(4)(12) states that the recipients of the Individual Electronic Health Record data, according to the article 4(9) of the GDPR, include the family doctor of the data subject, the treating physician, dentist or other health professional, during the hospitalization or the visit to a public or private health care unit, for the purpose of providing health services, as well as health professionals and public authorities, for the purpose of fulfilling a public interest in the field of public health. Law 4600/2019, Article 83(1) and Article 84(4)(5) as described above apply. In addition, Article 83(2) states that during the establishment and operation of each of the above-mentioned Registries by the Ministry of Health, who is the controller, the protection of human rights, privacy and the protection of personal data must always be ensured, in accordance with Article 9A of the Constitution and the current legislation and, in particular, in accordance with the provisions of the GDPR 2016/679. **Law 4624/2019**, Article 22(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, 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.
Legal basis GDPR	• 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	**Law 3984/2011**, Article 66(16) states that the treating physician, for reasons of personal data protection, is responsible for requesting from the patient, or if this is not possible, from a first-degree relative, the signed approval for the use of Telemedicine services. If this is not possible, then the treating physician uses Telemedicine services at his discretion. The instructions of Hospitals and Health Units which provide Telemedicine services are advisory and in no case mandatory. **Law 3892/2010**, Article 6(1) states that the General Secretariat for Social Security creates and operates an electronic prescription database. "(...) Each prescription and referral, shall be registered in it and shall have the content mentioned in Article 3 .(...)" All other information required for its operation are registered, such as the prices of medicines and services, data of the users to whom access to the e- prescription

	system is allowed, data of the Social Insurance Institutions, of the units that provide health services, or other units that provide services or benefits to insured people, suppliers of medicines and materials, as well as other data managed by the e-prescription system. Article 6(5) states that the creation and compliance of the e-prescription database is realised without prejudice to the provisions of **Law 2472/1997** "For the Protection of the Individual From the Processing of Personal Data", as in force. The General Secretariat for Social Security and the e-Government Center for Social Security Service SA (IDIKA SA) take all appropriate and proportionate to the risks, technical and organizational measures for the security of infrastructure, information systems and data and their protection against accidental or unlawful destruction, accidental loss, deterioration, prohibited dissemination and any other form of unauthorized processing or unlawful and authorized access and use. Law 4600/2019, Article 84(4)(2) states that the Individual Electronic Health Record contains the individual health history of the recipient of health services, as described above. Recently some other laws have been adopted. Joint Ministerial Decision 2650/2020 that regulates more specific technical issues for the operation of the National Patient for COVID-19; and Law 4722/2020, Article 12 par. 1 and 2 that regulate what data can be accessed by EODY, have been mentioned above. Law **4704/2020,** Chapter 2 'Digital public services through unified digital portal of public administration', Art 13 'Inmaterial operation of the system of electronic prescription of medicines', par. 2 states that the patient can log in to the Primary Health Care System (…) and declare that he wishes to receive electronically the prescription of medicines that are prescribed to him and the way in which he will receive the above prescriptions, which can be either via text message (sms) on his mobile phone (...), or via message (email) in his e-mail address, (…). **Law 4737/2020** article 31 par. 4 and 5 as amended by article 88 of **Law 4745/2020**: By joint decision of the Ministers of Health and Digital Governance, a district Database of Epidemiological Tests is established which is connected but distinct to National Patient Registry COVID-19. In this database, data of persons tested by the rapid molecular tests are registered.
Legal basis used for processing app or device derived data in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	Greece has specific regulations for genetic testing. Article 4 of **Government Gazette 4875/B/29-12-2017** on Preimplantation Genetic Diagnosis (PGD), states that PGD laboratories are housed in independent spaces within Medical Assistant Reproduction Units or operate outside the Medical Assistant Reproduction Unit and collaborate scientifically with it. The laboratories are licensed by the National Authority for Medically Assisted Reproduction, which checks whether the legal requirements are met. PGD laboratories operate with high quality standards and quality control procedures as defined by international organizations, guidelines and protocols of international and scientific companies, EU rules and decisions of National Authority for Medically Assisted Reproduction. PDG laboratories implement a quality system and update it. The certification is based on the ISO 15189 standard and is provided within two years from the licensing of the laboratory. The certification is carried out by the bodies accredited by the National Accreditation System. Additionally, the processing of genetic data for health and life insurance purposes is prohibited, as regulated in the article 23 of the Law 4624/2019, that has implemented the GDPR and the Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA into Greek Legislation.

8-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	**Law 3235/2004**, Article 10 (3) on Primary Health Care stipulates that for the carrying out of epidemiological, medical, financial, statistical and other relevant analyses and for the evaluation of services offered to citizens, the use of data from the electronic medical records is allowed after the consent of the citizen or without it, as long as their identity is not made public. **Law 2600/2019**, Article 84 (4) (10) states that the IDIKA SA, as the processor of the archiving system of Individual Electronic Health Record, is allowed to provide anonymous data to the Ministry of Health, in order to carry out epidemiological, statistical, financial, administrative and management analyses for improving the health and quality indicators of the services provided. Joint Ministerial Decision 2650/2020 regulates more specific technical issues for the operation of the National Patient for COVID-19.
Legal basis GDPR	• Other combination: 6(1)(a) Consent +9 (2)(i) public interest
Specific legislation addressing 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.	
National legislation	Greece has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	The Regulation 2017/745 on medical devices will apply from 26 May of 2020. Greek legislation regarding medical devices: • Government Gazette 2198B/2.10.2009 Ministerial Decision DY8Dd/130648/2009 on harmonization of the Greek legislation with the Directive 93/42 on medical devices, imposes certain requirements, such as chemical and biological characteristics, EC declaration of conformity, specific manufacturing prerequisites and CE mark. • Government Gazette 2197B/2.10.2009 Ministerial Decision DY8d/GPoik130644/2009 on active implantable medical devices, • Government Gazette 1060B/10.8.2001 Ministerial Decision DY8d/oik3607/892 on in vitro medical devices Law 4600/2019, Article 83 (1) (see above) states that by decision of the Minister of Health, National Patient Registries can be established and operate on the basis of specific criteria each time, such as (…) the purposes of pharmacovigilance. (….) Article 83 (3b) states that sensitive personal data collected and further processed in the context of each of the National Registries, which are established and operated in accordance with the provisions of paragraph 1, may be exceptionally processed, provided that there is at least one from the following cases: (b) Processing is necessary on the grounds of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and medicines or medical products, in accordance with

	the EU law or national provisions, which provide for appropriate and specific measures to protect the rights and freedoms of the data subject, in particular professional secrecy.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 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 • Other combination: 6(1)(a) Consent
Specific legislation addressing 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**	
National legislation	Law 4600/2019, Article 84(4)(4)(b) states that one of the conditions under which the processing of sensitive data, collected and processed in the context of the Individual Electronic Health Record, is allowed is if the processing is necessary for the public interest in the field of public health, such as protection against serious cross-border health threats or the ensuring of high standards of quality and safety of healthcare and medicines or European medical products, in accordance with EU law or national regulations, under the provision that appropriate and specific measures are taken to protect the rights and freedoms of the data subject, and in particular professional secrecy. Law 4600/2019, Article 83(1) (see above) states that by decision of the Minister of Health, National Patient Registries can be established and operate on the basis of specific criteria each time, such as the use of treatment in which the cost /the morbidity/ the mortality is increased, the high incidence of diseases in the general population, the use of specific treatment, the recording of rare diseases, the purposes of pharmacovigilance. Article 83(3b) as described above also applies. Joint Ministerial Decision 2650/2020 regulates more specific technical issues for the operation of the National Patient for COVID-19. **Law 4712/2020**, Article 77 regulates the emblematic action to tackle the virus SARS - Cov-2, as described below.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Law 4712/2020 Article 77: Regulations regarding the emblematic action to tackle the virus SARS - Cov-2 **1.** The **research centers** "Biomedical Research Foundation of the Academy of Athens" and "Institute of Applied Bioscience/ Centre of Research and Technology Hellas" and the university laboratories "Laboratory of Histology and Embryology /Dep. of Medicine/ NKUA and Laboratory of Hygiene, Epidemiology and Medical Statistics / Dep. of Medicine/ NKUA" participating in the Emblematic Research Action for the treatment of the virus entitled "Epidemiological study of SARS-Cov-2 in Greece through extensive tests for identifying the virus and antibodies, and sequencing of viral genomes and genetic analysis of patients for the treatment of the SARS-Cov-2 virus" *are allowed to have access to the data contained in the National Coronavirus Patient COVID-19*, established by the Ministry of Health and maintained by IDIKA SA. The coordinator of the Technical Project Monitoring Committee is defined as an accredited user who falls into the category "users for tracking purposes" of par. 5 of article 3 of joint Ministerial Decision no. 2650/2020 (B` 1298).  The personal data contained in the archiving system are used by the above entities and laboratories in order to fulfill the purposes of par. 3 of article 1 of **Ministerial Decision no. 2649/2020** (B` 1390). Their processing shall be carried out in accordance with the rules for the protection of personal data and in accordance with the provisions of Law 4624/2019.This processing is considered necessary for reasons of public interest in the field of public health and for scientific research purposes, in accordance with the purpose of the Partnership for the Project "Emblematic Action (…) ". The above entities and laboratories are given the opportunity to process this data in order to inform the subjects about the purposes of the Emblematic/Flagship Action and their participation in them and to use the personal data for the purposes of scientific research. **2.** To the research centers (…) "participating in the Emblematic Action (…)" 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 are transmitted in order to perform virome analysis and to confirm the diagnosis by immunological methods. In case of scientific research, in addition to the	

above mentioned, the patient is informed and consent is obtained.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 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
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	Law 4600/2019, Article 83 (3) states that the sensitive personal data, collected and further processed in the context of the National Patient Registries, which are established and operate, in accordance with the provisions of paragraph 1, is exceptionally permitted to be processed, provided that at least one of the following cases occurs : (a) the processing is necessary for the purposes of preventive or professional medicine, medical diagnosis, health or social care or treatment or management of health and social systems and services under EU law or national law or in accordance with the contract of a health professional, without prejudice to the conditions and guarantees mentioned in Article 9(3) of the GDPR, (b) Processing is necessary on the grounds of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and medicines or medical products, in accordance with the EU Law or national provisions, which provide for appropriate and specific measures to protect the rights and freedoms of the data subject, in particular professional secrecy, (c) the data subject has provided his written consent for the processing of such personal data for one or more specific purposes, unless EU law or national regulations provide that the prohibition of the processing of sensitive personal data cannot be lifted by the data subject, (d) the processing is necessary to protect the vital interests of the data subject or other natural person, if the data subject is physically or legally unable to consent, (e) the processing is, in accordance with EU law or national regulations, necessary for reasons of substantial public interest, which is proportionate to the intended purpose, respects the essence of the right to data protection and provides appropriate and specific security measures to ensure the fundamental rights and interests of the data subject, (f) the processing is necessary for archiving purposes on the grounds of the public interest, for scientific or historical research purposes or for statistical purposes, in accordance with paragraph 1 of Article 89 of the GDPR, under EU law or national regulations, which are proportionate to the intended purpose, respect the essence of the right to data protection and provide appropriate and specific measures to ensure the rights and interests of the data subject. In addition, as mentioned above the Joint Ministerial Decision 2650/2020 regulates more specific technical issues for the operation of the National Patient for COVID-19. Law 4737/2020 article 31 par. 4 and 5 as amended by article 88 of Law 4745/2020: establishes the Database of Epidemiological Tests which is connected but distinct to National Patient Registry COVID-19. In the above database, data of persons tested by the rapid molecular tests are registered. Operation of Patient Registries for other illnesses are the Cystic fibrosis Patient Registry (Ministerial Decision 4865/2020), Diabetes Patient Registry, and Hepatitis C Patient Registry.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the field of public health • 6(1)(c) legal obligation + 9(2)(h) healthcare • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: Law 4600/2019, Article 83 (4) states that the persons who, under the direct supervision of the Ministry of Health, which is the controller, or on behalf of the

	processor, that may be appointed by the controller - the Ministry of Health - are authorized to process the personal data contained in the national Registers, are bound by compliance with data privacy or confidentiality, regarding the performance of their duties in accordance with the relevant provisions, and in particular with the Code of Medical Ethics, the Civil Code and the Penal Code.

* Note. 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.

8-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Greece has no specific legislation on this topic.
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.	Greece has no specific legislation on this topic.

8-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Greece the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Greece:	
Mechanism	• Application to a local research ethics committee or IRB
There are no exemptions to the principle that the research must first be submitted to the application body.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Greece did not adopt such a system.	
Legislation has been adopted 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	
Greece has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	

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 the 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)(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 states that research centers participating in the Emblematic Research Action for the treatment of the virus entitled "Epidemiological study of SARS-Cov-2 in Greece through extensive tests for identifying the virus and antibodies, and sequencing of viral genomes and genetic analysis of patients for the treatment of the SARS-Cov-2 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 consent must be obtained.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Greece has no specific legislation on this topic.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
There are efforts within research projects where scholars exchange patient data for research purposes. But these are fragmented and are conducted within the realm of small pilots. Law 4712/2020, Article 77(2) (Regulations regarding the emblematic action to tackle the virus SARS - Cov-2) states in paragraph 2 that the patient's consent is required.

8-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Greece.

Rights of the patient	How the right can be exercised in Greece
Article 15 'right to access data concerning him or her'	• Through a formal national data access request system established by legislation
Law 3418/2005 (Code of Medical Ethics), Article 14 (8), as codified by article 99 of the presidential decree 28/2015 on access to public documents, states that the patient has the right to access the medical records, as well as to obtain copies of his file. This right, after his death, is exercised by his heirs, as long as they are relatives up to the fourth degree. Paragraph 10 of the above article states that the patient has the right to access, to the national or international records in which the personal data concerning him have been entered, in accordance with the relevant provisions. Also, Law 4600/2019 Article 84 (4) (12) states that as far as the data collected in the context of the Individual Electronic Health Record are concerned, the recipient of health services, who is the data subject, has, after the activation of the Individual Electronic Health Record, the right to access the information contained in it, in accordance with the provisions of article 15 of the General Data Protection Regulation.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Greece has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten'	• No, a patient may not delete his or her medical

May a patient have medical records deleted?	record
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

8-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Greece to include data from apps and devices in the EHR. In addition, the table displays how Greece have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
No, there are no such ICT systems Currently, there are attempts, towards the new cloud based EHRs where the patient has the right to ask from the doctor to download all of his/her medical data (in US it is called Blue button, in EU it is an obligation of EHRs to provide such kind of function due to the GDPR regulation). There are efforts like the clinic.iwelli.com that provide the patients the ability to download all of their medical data.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• 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. Patient generated data (Real world data) are subject to questioning of their quality and credibility. Also still there are no evidence-based protocols of their value towards the development of a medical plan. At the moment it is better to keep these data in a separate space away from the medical data of an EHR.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Greece does not yet participate in eHDSI but plans to do so by 2025.	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability
Greece participates in programs (within funded EU projects) to apply and validate interoperability protocols for medical data like the HL7 v3 / epSOS standard (CDA) for medical data exchange.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There are several national data security policies which address use of security standards in each healthcare provider sector (primary, secondary, tertiary, long term care)
The security policies have to do with the security of the cloud based services such as HTTPS protocol with data encryption protocol in TLS 1.2, two factor authentication method and others.	
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	

Policy level	• There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
The national data quality policy adheres to GDPR regulation principles	
Agencies which oversee the implementation of technical standards	
The Helenic Data Protection Authority oversees the implementation (https://www.dpa.gr/).	

8-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	Electronic Health Record http://www.idika.gr/pfy/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%BF%CF%82-%CF%86%CE%B1%CE%BA%CE%B5%CE%BB%CE%BF%CF%82-%CF%85%CE%B3%CE%B5%CE%B9%CE%B1%CF%82-%CE%B7%CF%86%CF%85.html
Hospital and medical specialist care	Covid-19 Patient Registry: https://covid19.gov.gr/ilektroniko-mitroo-asthenon-covid-19/
Prescription drugs	https://www.e-syntagografisi.gr/e-rv/p

9 COUNTRY FICHE SPAIN

The following sections provide an overview of the rules for processing of health data currently in place in Spain both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[11]

9-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The Additional Disposition 17 of the Organic Law 3/2018, of 5 December, on the **Protection of Personal Data and the Guarantee of Digital Rights** states that the processing of health and genetic data regulated in the following laws are the implementing provisions (among others) covered by letters (g), (h), (i) and (j) of Article 9(2) GDPR: • Law 14/1986, of 25 April, **General Healthcare Law**, establishes the general framework of the rights of individuals to health protection. • Law 31/1995, of 8 November, on the **Prevention of Occupational Risks**, provides for the processing of data for the purpose of promoting health in the workplace. It should also be mentioned: • Law 41/2002, of 14 November, **Basic Regulation of Patient Autonomy and of Rights and Obligations Regarding Clinical Information and Documentation** is the most relevant law in relation to the processing of data in the context of health care. It regulates duties and rights concerning clinical records and other clinical documents. It is a basic law that has been developed by the Autonomous Communities, which have competence in health matters (the substantial content does not vary significantly with regard to rights and duties concerning clinical documentation). • Law 16/2003, of 28 May, on the **Cohesion and Quality of the National Health System** provides that clinical records will be accessible in order to guarantee health care to patients throughout the national territory. • Law 14/2007, of 3 July, on **Biomedical Research**. Despite its title, it regulates the practice of clinical genetic analysis in its title V. It contains some particularities in relation to the processing of health data in general. • Law 14/2006, of 26 May, on A**ssisted Human Reproduction Techniques**. It regulates the processing of data on donors and users when assisted reproduction techniques are used. Please note there is no reference to article 6 GDPR in the Spanish Law that develops the health data processing. The reference is to article 9(g), (h), (i) and (j).
Legal basis GDPR	• 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 • Other combination: the legal basis for this data processing is established in 6(1)(b) for private health insurance entities, and in 6(1)(c) for public health.
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare	

[11] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Spain. The authors of the report take full responsibility for any interpretations in the country fiche.

provision purposes	
National legislation	Article 16(1) of the Basic Regulation of Patient Autonomy and of Rights and Obligations Regarding Clinical Information and Documentation states that the medical record is an instrument designed primarily to ensure adequate care for the patient. The centre's care professionals who carry out the diagnosis or treatment of the patient have access to the patient's clinical history as a fundamental instrument for adequate care. Article 56 of the Law on the Cohesion and Quality of the National Health System regulates the exchange of health information between bodies, centres and services of the National Health System: With the aim of ensuring that citizens receive the best possible health care in any centre or service of the National Health System, the Ministry of Health and Consumer Affairs will coordinate the mechanisms for the electronic exchange of clinical and individual health information, previously agreed upon with the Autonomous Communities, to allow both the interested party and the professionals participating in the health care to access the clinical record in the terms strictly necessary to guarantee the quality of said care and the confidentiality and integrity of the information, regardless of the Administration providing it.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care • Other combination: the legal basis for this data processing is established in 6(1)(b) for private health insurance entities, and in 6(1)(c) for public health.
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Spain has no specific legislation on this topic. Regions (namely Autonomous Communities) hold the competencies on health care provision, including for providing any digital health services, therefore the regions are the competent governance level to regulate this issue.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) health or social care
Specific legislation on **genetic testing**	
National legislation	Spain has specific regulations for genetic testing. There is a specific regulation for carrying out genetic diagnosis in articles 46 to 57 of the Law on Biomedical Research. In particular, with regard to quality requirements, according to Article 56 "The entire process of genetic counselling and genetic analysis practice for health purposes must be carried out by qualified personnel and must be carried out in accredited centres that meet the quality requirements established by regulations for this purpose." In addition, Article 57 states that the competent regional or state authority shall accredit the centres, whether public or private, that can carry out genetic analyses. **Order SSI/2065/2014**, of 31 October, amending Annexes I, II and III of Royal Decree 1030/2006, of 15 September, which establishes the catalogue of common services of the National Health System and the procedure for updating it, refers to the above-mentioned articles.

9-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Article 16.5 of of the Basic Regulation of Patient Autonomy and of Rights and Obligations Regarding Clinical Information and Documentation states that "Duly accredited health personnel who carry out inspection, evaluation, accreditation and planning functions have access to clinical records in the fulfilment of their duties to check the quality of care, respect the rights of the patient or any other obligation of the centre in relation to patients and users or the health administration itself." Article 18 of the General Health Law states that "the Public Administrations, through their Health Services and the competent bodies in each case, will develop the following actions: (...) 16.The control and improvement of the quality of health care at all levels." Article 69.2 the General Healthcare Law states that "The evaluation of the quality of the care provided shall be a continuous process that shall inform all the activities of the health personnel and health services of the National Health System. The health administration will establish care quality evaluation systems after hearing the scientific health societies. Doctors and other qualified professionals of the centre must participate in the bodies in charge of evaluating the quality of care of the centre."; and 69.3 "All Hospitals shall enable or facilitate external quality control units to carry out their tasks. Likewise, they shall establish the appropriate mechanisms to offer a high level of care quality." The Law on the Cohesion and Quality of the National Health System also develops the quality accreditation systems, as an obligation of the Public Administrations. Furthermore Law 33/2011, of 4th October, **General Law on Public Health** establishes users of health information for public health including epidemiology among others. And the Organic Law 3/1986, of April 14, on **Special Measures in the Field of Public Health** is also relevant.
Legal basis GDPR	• 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 (in the case of a public body exercising official authority) • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health • Other combination: 6(1)(b) performance of a contract+ Art.9.2 h (contract with a health professional)
Specific legislation addressing 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.	
National legislation	Spain has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Law 29/2006, of 26 July, on **Guarantees and Rational Use of Drugs and Health Products** establishes the guarantees for monitoring the risk-benefit ratio of drugs and regulates the Spanish Pharmacovigilance System and the pharmacovigilance of drugs for human use. The **Royal Decree 577/2013**, of 26 July, regulating the pharmacovigilance of medicines for human use, develops this provisions and establishes the obligations of the institutions involved in the pharmacovigilance process (Autonomous Communities and the Spanish Drug Agency), health professionals, and the holder of the commercialisation authorisation for the drug. The sources of the data are described. Post-authorization studies are regulated. These studies are not exactly pharmacovigilance, but their purpose is to complement the information obtained during the clinical development of the drugs prior to their authorization. The regulation of these studies is developed in the **Royal Decree**

	957/2020 of 3 November (entering into force 2 January 2021, regulating observational studies with medicines for human use. In this case the consent of the subjects is required unless the Ethics committee considers a signifcant social value of the study and and it cannot be feasible or viable without such a waiver, and that it entails minimal risks for the participants; or other legal basis is applicable. .
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • Other combination: 6(1)(a) consent and 9(2)(a) consent • Other combination: 6(1)(e) public interest and 9(2)(j) research purposes
Specific legislation addressing 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**	
National legislation	Spain has no specific legislation on this topic. However, the general legislation covers that scenario: It is legitimate to access medical records for epidemiological purposes (article 16 of Law 41/2002), and according to Law 33/2011, of 4th October, General Law on Public Health, cooperation and solidarity are the main preventive actions, so public health in any territory cannot be addressed without considering international action as an integral part of national public health policy. Article 39 of this law (Actions in international health): 1. "In matters of international health, the Ministry of Health, Social Policy and Equality shall exercise the following actions: (...) b) Collect information on health risks of an international nature and inform the General State Administration bodies responsible for coordinating emergencies and civil protection." From a more general perspective, according to article 3 of the Organic Law 3/1986: In order to control communicable diseases, the health authority, in addition to carrying out general preventive actions, may adopt appropriate measures for the control of the sick, of persons who are or have been in contact with them and of the immediate environment, as well as those considered necessary in the event of a risk of a communicable nature.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. The Ministry of Health coordinates the notification control system and there is a National Public Health Surveillance Network (RENAVE) that articulates surveillance by integrating the notification and epidemiological investigation of cases of communicable diseases. The general regulations are contained in the General Law on Public Health. It is possible that data are transmitted from the laboratories directly to institutions dealing with communicable diseases, but procedures are articulated by each autonomous community.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Spain has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	In Spain, there are two kinds of registries. Those created by the public authorities and those named "clinics", created by health professionals. The registries created by the authorities are based on the public interest in the field of public health. See Article 23 of the General Healthcare Law, and Article 41 of the General Law on Public Health. Those "clinics" are based on the consent of patients.
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(i) public interest in the field of public health • Other combination: 6(1)(a) consent+ 9(2)(a) consent
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • Other: It depends on each registry. In case of health authority registries, those with

	responsibilities in the management of health care can access. In the case of clinical registries, it is different. They are fed with data from the patients themselves or from professionals and also have the research dimension.

* Note. 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.

9-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Spain has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes
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.	Spain has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes
National legislation	In Spain, the legislation does not differentiate between not for profit researchers and for profit researchers. The following legislations apply. Law 41/2002, modified by OL 3/2018 states that: Article 16(3). Access to medical records for (...) research purposes (...) is governed by the provisions of the legislation protection of personal data and of the Law 14/1986 (…). Access to the medical record for these purposes requires the preservation of identificative data of the patient, separated from those of clinical character, in a way that, as a general rule, anonymity is ensured, unless the patient has given his consent not to separate them. Exceptions are made for the cases of research foreseen in section 2 of the Additional Provision 17ª of the OL 3/2018 (...). The Additional Provision 17a.2 describes a) The re-use of personal data for biomedical research purposes; and b) The use of pseudonymised personal data for research in biomedical research. ALaw 14/1986, the General Healthcare Law states that ." Article 9 (Duty of communication) and Article 50 (Promotion of research in public health) are also relevant. The sixth transitional provision of OL 3/2018 also provides that re-use of data collected before the entry into force of this law for health research purposes will be considered lawful when any of the following circumstances are : a) Those personal data are used for the specific purpose for which the patient have given consent. b) That, having obtained consent for a specific purpose, the data are used for research areas related to the medical specialty in which the initial study was scientifically integrated. Law 14/2007 on Biomedical Research explains the procedure to get approval from an Ethical Review Board/ERB. ERB authorisation applies to all types of research bodies.

9-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Spain the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Spain:	
Mechanism	• The data controller provides direct access upon proof of agreement of a research ethics committee or DPA • Other: upon compliance with the research ethics committee requirements and procedures
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Spain did not adopt such a system.	
Legislation has been adopted 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	
Spain has no specific legislation on this topic. It is worth noting that stemming from the Transparency Law there is a regulatory body on Open Data that specifically includes the purpose of research. Additionally, main public competitive research calls include provisions on Open Science and Open Data publication within the project requirements.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Spain did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Spain has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
There are several sector specific regional systems to share data for secondary use.	

9-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Spain.

Rights of the patient	**How the right can be exercised in Spain**
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Spain has not adopted specific legislation on the application of such a right in the area of health.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Spain has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions

There is an obligation to maintain clinical information for a minimum of 5 years from the date of discharge. During this period, clinical data may not be deleted, stated in Article 17.1 of the Basic Regulation of Patient Autonomy and of Rights and Obligations Regarding Clinical Information and Documentation.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR (according to article 17 of the Organic Law 3/2018)

9-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Spain to include data from apps and devices in the EHR. In addition, the table displays how Spain have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
• This is organised nationally. • This is organised regionally. Patients have the possibility to access to their information by three means: 1) NHSEHR system which allows to access clinical reports generated within all regions in which the patient received healthcare or treatment. 2) Carpeta ciudadana, which is a system at national level within public administration related to the strategy of electronic administration that allows citizens the access to the information hold by public administration from a cross-sectorial point of view (health, taxes, etc.) 3) Regional ICT systems in which the patient can access clinical reports generated within the region in which they are afiliated.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	Within the NHSEHR there is no such possibility. However at regional level, ICT Systems used by regions in some cases may allow to integrate mHealth (Personal data collected through Apps) with the EHR.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Spain will participate in eHDSI with Patient Summary and ePrescriptions, as this is already in place at national level with the system NHSEHR and the NHS for ePrescription which allows the exchange of ePrescriptions through all the territory. The participation in this EU projects is a natural step for the National Health System (NHS).	
Technical standards	
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	
Policy level	• 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) • 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)
There is a National Interoperability Framework for the electronic administration: Royal Decree 4/2010, of 8 of January, on the **National Scheme of Interoperability in the field of e-administration**. The Framework includes the criteria and recommendations for security, standardisation and conservation of information, formats and applications. The National Interoperability Framework sets the adoption of interoperability standards through the work of a	

National Technical Committee (CTN) with differentiated charters and workgroups for each area of interest. There are currently 191 regulations regarding interoperability standards in effect.

CTN139 for Information and Communication Technologies in Healthcare is responsible for the adoption of interoperability standards in healthcare information systems and electronic health records, messages and communication within healthcare administration, semantics, ontologies and health knowledge base, and healthcare devices and national health system insurance identification (health insurance card). CTN 139 coordinates at the European Level with CEN/TC 251 and at international level with the ISO/TS 215 about healthcare information.

Main interoperability standards in use in Spain regarding health data are:[12]

- **Organizational interoperability**: ISO 13940
- **Semantic interoperability**: UNE-EN-ISO 13606:2; IHE profiles; SNO MED-CT; ICD (from 2016 onwards ICD-10-MC ES); LOINC (laboratory); SERAM (medical imaging)
- **Syntactic Interoperability**: UNE-EN-ISO 13606:1; DICOM; HL7/FHIR; ASTM
- **Technical interoperability**: XML, SOA, TCP/IP; Web Services, HTTP REST

Additionally, there is a NHS Interoperability Framework developed by the Ministry of Health in accordance with the Regional Health authorities to enable the exchange of information on the Health Insurance Identification (Health Card User Database), the NHS Cohesion Fund, on ePrescriptions, Medical History (EHR extract) and other health care and administrative services across all NHS. Besides this, **Royal Decree 1093/2010** establishes the terminologies and data structure of the NHS clinical reports.

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care) • Each region has one data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

There is a National Security Framework (ENS) for the electronic administration (Royal-Decree 3/2010, and further developed at Royal-Decree 951/2015 on the **National Security Scheme in the field of e-administration**) that includes the basic principles and minimum requirements for adequate information protection and that is applied by public administrations to ensure the access, integrity, availability, authenticity, confidentiality, traceability and conservation of data, information and services used in electronic media that they manage in the exercise of their powers.

Information and communication technologies security policies, procedures, regulations and technical instructions are under the responsibility of the National Center for Criptology (CCN-CERT), adscript to the National Intelligence Center (CNI) that produces specific guidelines related to information security issues (series 800 guidelines for the ENS), including those involving health data security policies.

Additionally, there is a national Health Information Security Policy issued by the Ministry of Health (Order SSI/321/2014 on the **NHS Information Security Policy in the field of e-administration**) regulating the scope and specific objectives in the application of the National Security Framework to health data security and establishing the structure to enforce its compliance through the NHS Information Security Committee and information security roles within the health administration.

Main information security standards in use in Spain regarding health data are UNE-ISO/IEC 27001 and UNE-ISO/IEC 27002.

Finally, Autonomous Communities could have their own Health Information Security Policies extending or complementing the national Health Information Security Policy depending on the development of their health and care information systems and the particularities of the health administration organisation in the regions.

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

[12] From publication "Manual práctico de interoperabilidad semántica para entornos sanitarios basada en arquetipos". Instituto de Salud Carlos III. Ministerio de Economía y Competitividad, June 2013.

Policy level	• There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

The National Statistics Institute (INE) is responsible for maintaining a national data quality assurance framework regarding all statistical data including health and healthcare data. The national quality assurance framework is inspired by the prevailing schemes at international level, such as that of the United Nations or that defined by Eurostat on the basis of the European Statistics Code of Practice (ESS).

Additionally, the Ministry of Health includes public health and healthcare information systems within the overall Quality Plan for the NHS issuing technical and methodological guidelines for health data management in the context of monitoring population health and NHS performance (key indicators of the NHS).

Agencies which oversee the implementation of technical standards

The National Statistics Institute (INE) oversees the implementation of the data quality standards over all national statistics, including health and healthcare data.

The Ministry of Health oversees the implementation of the data quality standards over health and healthcare data statistics at the national level, and each region is responsible for the data quality of their health information systems.

Other bodies such as the Institute of Health Information (with a role on interoperability), the National Intelligence Center (CNI) or the Spanish National Cybersecurity Institute (INCIBE) both with a role on security and the Spanish Data Protection Agency (AEPD) on privacy.

9-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	Primary Care Clinical Database – BDCAP (Ministry of Health) https://www.mscbs.gob.es/estadEstudios/estadisticas/estadisticas/estMinisterio/SIAP/home.htm
Hospital and medical specialist care	Registry of Variations of Medical Practice in the National Health System (AtlasVPM) (IACS) https://www.atlasvpm.org/ Registry of Resources and Quality of Care in the Clinical Units of Cardiology (RECALCAR Registry) (Spanish Society of Cardiology) https://secardiologia.es/institucional/reuniones-institucionales/sec-calidad/recalcar Joint Database of the Spanish Network of Cancer Registries (REDECAN) Spanish Registry of Childhood Tumors (RETI-SEHOP) https://www.uv.es/rnti/ Registration of Nosocomial Infection in Intensive Care Units (ENVIN) (Spanish Society of Intensive and Critical Medicine and Coronary Units (SEMICYUC) - Spanish Foundation for the Critically Ill (FEEC)) https://semicyuc.org/envin/ Registry Database of the Spanish Network of Hospital Costs (RECH) (MAR Institute of Medical Research Foundation (IMIM)) https://www.rechosp.org/rech/faces/es/jsf/index.jsp Acute Myocardial Infarction Delay Analysis Record (ARIAM) (Spanish Society of Intensive and Critical Medicine and Coronary Units) https://semicyuc.org/ariam/ Spanish Fertility Registry (Spanish Society of Fertility) http://www.cnrha.msssi.gob.es/registros/home.htm
Prescription drugs	Primary care medical records database for pharmacoepidemiological studies – BIFAP (Spanish Agency for Medicines and Healthcare Products (AEMPS)) http://www.bifap.org/

10 COUNTRY FICHE FRANCE

The following sections provide an overview of the rules for processing of health data currently in place in France both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[13]

10-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	Since the **Act on patients' rights** *[Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé]* many specific laws have been adopted regarding healthcare services organisations and practices which include references to personal data processing for healthcare purposes. All legal provisions have been integrated within the **Public Health Code (PHC)**. The Code also refers to the **French Data Protection Act (LIL)** *[Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modified]* regarding specifically personal health data processing and protection rules. Summary of main legal basis fixing rules for personal data processing for healthcare: • For healthcare provision by hospitals and liberal physicians and health services administration: Art. 44(1) LIL, Art. 9(2)(a), (c)-(f) GDPR; Article L. 1110-4 and 6113-7 PHC; • For ensuring social security services and complementary activities from health insurances: Article L114-12-4 and L. 114-22 Social Security Code (SSC); • For ensuring healthcare coordination, in particular through the patients' Shared Medical Record (DMP): Art. L. 1111-15 PHC; • For health services management and health monitoring by the Regional Health Agencies, by States Health Agencies and Authorities: Art. L. 6113-8 PHC. Medical Deontology Code, which is included in the PHC, prepared by the National Order of Physicians (CNOM) must be respected by physicians as specified under Art. R.4127-1 PHC. This includes the respect of medical secrecy and of confidentiality of the data. Most of the provisions regarding the processing of Health Data are sanctioned under the French Penal Code (e.g., breach of professional secrecy, lack of information etc.). In addition, provisions can be the basis for sanctions by the administrative and civil courts, and professional orders (the latter only for disciplinary sanctions).
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent • 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Article L. 1110-4 PHC allows the sharing of personal data necessary to provide care to the patient, to ensure healthcare coordination, continuity or medico-social follow-up of the patient under several conditions. Articles L. 1110-4-1 and L. 1110-4-2 PHC details security and confidentiality measures to be respected in order through information systems used to communicate personal health data.

[13] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in France but the authors take full responsibility for any interpretations in the country fiche.

	Article L. 1111-8 PHC fixes a mandatory certification system applying to any third subcontracted personal health data hosts which intend to store personal health data collected within the health system at the occasion of healthcare provision, of prevention, diagnostic or medico-social follow-up. The certification is performed by the specialised unit of the French Agency of Shared Information System (ASIP-Santé). Articles L. 1111-14 to L. 1111-24 and R-1111-26 to R. 1111-43 PHC regulate the DMP (Dossier Médical Partagé). Articles L. 1111-18 and L. 1111-19 PHC, together with Articles R. 1111-40 to R. 1111-43 PHC regulate the access to the data contained within the DMP. The personal health data will be stored for as long as required under the French law, in particular for complying with Articles R. 1112-7 PHC regarding the storage duration of patients medical records.
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent • 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Regarding telemedicine: Article 78 of the *Loi n°2009-879* on the hospital, patients, health and territories defines telemedicine for the first time (Art. L. 6316-1 PHC). Five telemedicine acts are defined in Decree n°2010-1229 of October 19, 2010 as well as their conditions of implementation. The acts (Article R. 6316-1 PHC) are: 1) Teleconsultation; 2) Tele-expertise; 3)Medical telesurveillance; 4)Remote medical assistance; and 5) Medical response which is distributed within the framework of the medical regulation mentioned in Article L. 6311-2 and in the third paragraph of Article L. 6314-1 PHC. Other texts apply such as the LIL (data protection), the High Health Authority (HAS) Guidelines, the Agency for Digital Health (ANS) Guidelines and technical referentials, General Policy on Security of Health Information Systems - PGSSI- S, which supervise this medical practice to ensure the quality and safety of care and exchanges. Within this general framework Telecare, a specific form of telemedicine as referred to in Article L. 6316-2 PHC is subject to specific professional guidelines according to the medical speciality practiced through ICT.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent • Other: when the individual is no more able to consent, so in exceptional cases, the following legal basis applies: 9(2)(c) protecting the vital interests of the data subject or a third person.
Specific legislation on **genetic testing**	
National legislation	France has specific regulations for genetic testing.[14] Article 16-10 of the Civil Code restricts genetic testing for health purposes to medical or scientific research. With regard to patients' rights, Article 16-10 of the Civil Code and the PHC (Articles L. 1131-1 to 1131-7) are covering the prescription of genetic testing and are mentioning the core legal principles to be respected. With regard to professional practices the following legislation applies: • The *Loi n° 2013-442 du 30 mai 2013 portant réforme de la biologie médicale* establishes the rules for practicing genetic testing for medical purposes. • The *Arrêté du 27 mai 2013* fixes good practices for constitutional genetic testing practices in France, for medical purposes. The Haute Autorité de Santé (HAS) issued guidelines in relation to the Arrêté. • Articles L. 6211-1 to L. 6242-5 PHC regulate the activity of laboratories practicing genetic testing for medical purposes in accordance with the previously cited acts.

[14] The legislations mentioned in this box are restricted to genetic testing in health and are not fully covering the use of genetic information for other purposes.

	• Articles L. 1132-1 to L. 1132-7 PHC regulate the profession of genetic counselor. Accreditation of laboratories able to perform genetic testing is mandatory since 2013.

10-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	According to the **Law related to the organisation and the transformation of the health care system** adopted in 2019 *[Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1)]*, the National System of Health Data (SNDS) is in charge of collecting personal health data for the needs of implementing and developing national policies. The current sources of the data to be included in the system are listed in the PHC article L. 1461-1-I. These data support the activities of the SNDS integrated into the Health Data Hub that are strictly mentioned in the PHC (Article L. 1461-1-III). The main mission of the SNDS is to share the Data in order to contribute to: 1. Information on health as well as on the supply of care, medical and social care and their quality; 2. The definition, implementation and evaluation of health and social protection policies; 3. The knowledge of health expenditure, health insurance expenditure and medico-social expenditure; 4. Inform health or medico-social professionals, structures and establishments about their activities; 5. Health surveillance, monitoring and safety; 6. Research, studies, evaluation and innovation in the fields of health and medico-social care. Strict conditions must be respected to ensure the respect of confidentiality and the professional secrecy. Personal health data must be strictly kept confidential and in the respect of their integrity and traceability, according to a referential referring to the LIL and the GDPR requirements. The law (Article L1461-5) strictly forbids the use of the SNDS data for the promotion of health products to health professionals and health care institutions and for the amendment of insurance contracts.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) healthcare • 6(1)(e) public interest + 9(2)(h) healthcare
Specific legislation addressing 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.	
National legislation	According to the LIL the processing of health data for research purposes including drug marketing authorisation and approvals for medical devices are falling under two sets of regulations. As for the processing and use of the data they are framed under the "Public interest" (6.1) provisions. The data subject needs to be informed about this use according to the LIL. Opt-out should be made possible, but will very unlikely be satisfied in such a

	case where public interest can overrule the individual right to oppose. Such activity of market approval is usually the last step of research on medicinal products or medical devices. As for information and consent for research activities, the applicable rules are those related to the conduction of research activities involving data from human beings (Article L. 1121-1 PHC and following) and must conform with information requirements under LIL/GDPR or MR003. As for in vitro medical devices performance the French National Agency has adopted a simplified procedure where applicants engage to respect the relevant methodology to conduct such processing (Methodology of reference, MR002).
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(i) public interest in the field of public health • Other combination: national legislation Article L. 1121-1 PHC and following and LIL
Specific legislation addressing 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**	
National legislation	The pharmacovigilance system is organised at regional and national level according to articles L. 5122-5, L. 5121-22 to L. 5121-26 PHC, and R. 5121-150 to R. 121-201-8 PHC. The information collected for pharmacovigilance purposes are those mentioned in Article R. 5121-151 PHC. The National Agency for Drugs and Medical Products Safety (ANSM) has adopted specific best practices guidelines (last update: 2018). Medical device safety is organised by the PHC at articles L. 5211-1 and R. 5211-1 to R. 5211-3. Several recommendations have been adopted by ANSM for specific medical devices. All the personal health data that is collected for vigilance activities should conform to standards elaborated by the CNIL. According to "Health vigilance standard" ("Référentiel") adopted by the CNIL on the 18th of July 2019: • The data controller must engage in the respect of this standard through a formal declaration of engagement on the website of the CNIL; • Prior starting the processing the data controller must conduct a Data Protection Impact Assessment; • Data are processed under the legal basis of legal obligation and public interest in the field of public health; • The individuals from whom the personal information is collected must be individually prior informed; • The standard bans any possibility to use genetic information in the context of pharmacovigilance and materiovigilance, if applicants want to use genetic information for the needs of their processing a specific authorisation must be requested to the CNIL.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • Other combination: GDPR and national legislation
Specific legislation addressing 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**	
National legislation	The main legal basis allowing the processing of health data for protecting against serious cross-border threats in the LIL is Article 67 which states that processing of health personal data in the case of health emergency are lawful if the controller has been previously identified in a list elaborated by the Health Ministry and the Social security Ministry after a positive opinion of the CNIL. This process should only respect the obligation of Personal Data Protection Impact Assessment and related consultation (section 3, Chapter IV of the GDPR). In the context of a COVID19 crisis, the following acts have been adopted in relation to the Sanitary Urgency main Act, the Loi n°2020-290, which allow and organise the secondary processing of personal and health data for fighting against the spreading of the disease, warn individuals about contact with infected persons and perform epidemiological studies related to this disease in the public interest: • Arrêté of 21 April 2020, allows exceptional collection of additional health and medico-administrative data for the sole purpose of helping research in the public health interest, for the management and resolving of the crisis. The categories of

	data concerned are listed under Article 1 of this Arreté. • Law n°2020-546 of 11 may 2020 Article 11, creates a special information system in the context of the crisis which is composed of two things: the SI-DEP (Screening Information System) and CONTACT COVID, a specific database which records positive tested patients as well as their close contacts for follow-up. Further details are provided within the application Decree n°2020-551.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Several health data can be communicated to the health surveillance authorities. In case of transmissible diseases that necessitate an urgent intervention at local, national or international level or for disease necessitating a surveillance in the name of the public health policy (article L. 3113-1 PHC), medical doctors and laboratories (either public and private) are reporting to the dedicated medical doctor and collaborators operating in the competent Regional Health Agency (Agence Régionale de Santé) which is representing the Ministry of Health. This is forwarded into a central database managed by Santé Publique France (the national agency for public health). According to the PHC (Articles R. 3113-1, R. 3113-2, R. 311-3, R. 3113-4 et R. 3113-5) a specific procedure of anonymisation of the data must be respected to transmit the information that are considered as confidential and protected under the professional secrecy. As for other types of surveillance (biological surveillance, resistance to pathogens etc.) a regional network is organised under the umbrella of Santé Publique France through National Reference Centres for the Control of Communicable Diseases (CNR) and in the name of the public interest. The PHC (articles L. 1413-3, R. 1413-46 and following) organises the transmission of the information which must be in accordance with the GDPR and the LIL requirements. At the European level, Santé Publique France is contributing to the surveillance effort through the contribution of several projects conducted by ECDC such as the European Antimicrobial Resistance Surveillance Network. This internal organisation allows the communication of relevant health information to European institutions in an anonymised way however, no possibility is legally offered, to date, to laboratories to directly communicate this data to European bodies.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	France has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	France has no specific legislation on this topic. However, the CNIL has issued not a legislation but a recommendation in order to facilitate the collection and use for public health interest of such data for cancer registries (Délibération n°03-053) and for rare diseases (Délibération n°2019-113). As for cancer registries or rare diseases registries included in the National Database information, individuals have an opt-out option, thus usually the legal basis for collecting personal health data in registries is not consent. As for the other types of registries (e.i pathology registry or child defects) either an informed consent or an information/opt-out mechanism could be required by the national authorities. Currently, a Methodology of Reference (MR) is under discussion at the CNIL in order to offer a more flexible and more global framework for future registries. In addition, a specific regulation is organising the collection of personal health data in the context of workers' health surveillance since 1985, Décret n°85-603, which is regularly updated.
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • Other: In France there is no global legislation covering the access to the data contained in registries. The access is regulated by each registry according to the principles of the LIL. In any case the access must conform to the objectives of a research program or for the needs of public health in the respect of the law. As a

	consequence nor employers nor insurance can have access and use personal health data.

* Note. 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.

10-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	France has specific legislation on this topic. Legal basis: • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
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.	France has specific legislation on this topic. Legal basis: • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
National legislation	In France, the legislation does not differentiate between not for profit researchers and for profit researchers. There are several provisions in the LIL and its implementation Decree n°2019-536 allowing and conditioning the further processing of personal data for scientific research by third-parties, whether public or private organisations, and establishing a unique regime for such processing for both types of legal entities. By principle: • Article 4(2) LIL on processing purpose limitation explicitly mentions that further personal data processing for scientific or historical research, for statistics, or for archiving purposes in the public interest shall be deemed compatible with regard to the initial processing purpose if compliant with GDPR and National law. • Article 4(5) LIL on storage limitation explicitly states that personal data can be stored for longer than the time necessary to meet the initial purposes provided that the data are processed exclusively for archival purposes in the public interest, for scientific or historical research, or for statistical purposes. The choice of data kept for archival purposes in the public interest is made under the conditions provided for in Article L. 212-3 of the heritage code (Code du Patrimoine). • A further processing should only be understood here where the personal data at stake are not collected directly with the data subject. To be lawful: • Article 6(II) LIL regarding the legal bases for the exceptions to the prohibition of sensitive personal data processing refers to those fixed under Article 9(2) GDPR. Any of these legal bases can be used for secondary personal data processing under the conditions previously mentioned and in the respect of professional secret, security, confidentiality and other data controller and processor obligations fixed under Title II Chapter III of the LIL. • Article 44 LIL specifies the list of legal bases provided under Article 9(2) GDPR, and includes in particular the processing necessary for public research within the

	meaning of Article L. 112-1 of the Research Code, provided that reasons of significant public interest make it necessary, under the conditions provided for by Article 9(2)(g). (Article 44(6) LIL) • Article 72 LIL states that conditions in which personal data processing whose purpose becomes research (i.e. secondarily) are framed according to Article 66-71 and 73-79 LIL. • Specific requirements under Article L.1121-1 PHC regarding research involving human beings shall be complied with where applicable to the type of research at stake for which data are planned to be reused (in particular regarding additional participant's information, consent to participation in the biomedical research etc.). The CNIL specifies that the consent provided under the PHC is restricted to the participation in a health research and does not legally base the processing of personal data in the meaning of the LIL.

10-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In France the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in France:	
Mechanism	• 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 and DPA approvals • Application to a centralised data governance and access body (E.g. SNDS, Cohorts) is possible (hence other than each data controller / data custodian individually)
Where required by law, applications are always necessary, even when the data are pseudonymised. Application to ethics review committees for research involving human beings (qualified under PHC rules) are set forth by law. This includes the setting up of a collection of human biological samples or a biobank. These committees, the Comités de Protection des Personnes (CPP) review personal data aspects and compliance elements regarding the LIL requirements. In addition to a CPP review, most of the researches will be able to comply with a CNIL MR, which requires a Data Protection Impact Assessment. Projects which do not comply with the scope and conditions of a MR will need to obtain CNIL authorisation. Research projects need to be followed by a DPO attached to the research promoter, if necessary in collaboration with other DPOs from participant organisations, which will monitor compliance of the project with the LIL. Applications to research ethics committees (CPP) are not mandatory for researches that do not involve human beings. However, if personal health data are being processed the researchers must comply with the LIL and, if applicable, to the specific CNIL MR004 applied to health research on data already collected. In practice, several IRBs are competent to assess and provide an opinion about such type of research, in particular for those projects involving publications of results in scientific journals. Their consultation is recommended. Applications to access data of the SNDS can include a mandatory evaluation of the project by the CESREES that must provide its opinion on the project. The CESREES is hosted by the Health Data Hub (HDH).	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
France did not adopt such a system. However, even though it cannot be qualified as altruism per se there is a possibility under the French law to collect personal health data in the context of a data warehouse. In that case, two procedures can apply depending on the policies of the applicants either the collection is based on consent or, if not, based on public interest. A data warehouse must be authorised by the CNIL.	

Legislation has been adopted 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
France has specific legislation on this topic. In 2016 France adopted the Law n°2016-1321 for a Digital Republic, where the principle of Open Data by Default has been adopted concerning public sector information. According to this law, public administrations of more than 3500 persons must publish their databases on the Internet, in the respect of anonymisation and the protection of intellectual property and industrial and commercial secrecy. Though not dedicated to research activities, this law applies to research as public research institutions and universities are covered. FAIR principles are not referred to in the law but the various provisions endorse them.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
There might be in the future. The Health Data Hub (HDH) incorporates various health data from different sources including data from patients (espace numérique de santé) which include the DMP. The data will be accessible for medical care only if the patient gives prior consent and in the respect of strict rules of security and confidentiality, it is still unclear if the data will be accessible for research purposes.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Article 30 Law n°2016-1321 states that 'No publication resulted from research funded at 50% rate by public institutions can fall under the Law for a Digital Republic'. Private research can only fall under this publication exception. There are guidelines for opening research data.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
• There are several national systems to share data for secondary use. • There are several sector specific regional systems to share data for secondary use. National systems to share data are the Health Data Hub (including the SNDS) and registries. Biobanks do not provide access at a national level but they have developed policies, that conform to the law on research and to the LIL, to provide samples and attached data for the needs of research. As for Biobanks the French legislation facilitates the reuse of the data through an opt-out system. In addition, several national cohorts provide access to their data (e.i. Constances, Elfe). In biobanks and for cohorts the usual procedures for granting authorisation are in place such as scientific and ethical evaluation of the projects, data access committees, and data transfer agreements.

10-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in France.

Rights of the patient	How the right can be exercised in France
Article 15 'right to access data concerning him or her'	• Other: According to the PHC patients have access to all their medical information through their right to be informed of their health status (Article L 1111-2). This provision specifies the LIL which grants a general right to access personal data.
For the medical record: If the patient wants to access his medical record a specific procedure must be followed in the respect of the PHC. The patient can be granted direct access to his medical record (Article L. 1111-7 PHC, Article R. 1111-1 and following), after ensuring his identity, by either a medical professional or the medical institution. In some cases and for specific claims the medical record can also be consulted by rights holders if the patient is deceased or by parents for minors. Medical professionals and medical institutions must respect a delay for the access that is stipulated	

by law. The consultation of the documents is provided for free if it is at the place of the medical exercise, if copies are sent to the patient they can be charged.

For the DMP: The DMP is currently deployed in France (Article L. 1111-14 PHC). This record is open by the patient on a voluntary basis with the aim of facilitating the access by professionals to shared medical information (Articles R. 1111-35 to R. 1111.39). Patients must authorise each professional that wants to include medical information in this record. The access is done directly by the patient through an electronic system (Username and login) allowing him to organise the information to be included in the record.

Article 16 'right to rectify any inaccurate data concerning him or her'	• 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) GDPR

For the medical record: the general right to rectification applies (article 50 LIL refers directly to article 16 GDPR). The patient, the rights holders or the parents, can access the medical record and ask for rectification. However, in practice this right can only be applied to "material" information (name, address etc.) or for a legitimate reason if medical information is concerned.

For the DMP: according to Article R. 1111-37 (PHC) the patient can ask either to the medical professional or to the national Health insurance to make the rectification, or he can directly make the rectification by himself. However, if the medical data has been reported by a medical professional the patient cannot directly erase the data, he can only ask for this erasure to the professional concerned or the medical institution which holds the data, for a legitimate reason.

Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record

Strictly speaking there is no right for deletion of the entire medical record. Patients can ask for erasing some information in case of legitimate interest but there is no possibility to delete the whole medical record.

The law has provided time limits for the conservation of the medical record by the institutions: 20 years for records held in public/private medical institutions after the last medical act and 10 years for the DMP after its closing. Other time limits are specifically mentioned in the PHC (e.g. data concerning minors). These are minimum time limits, public/private medical institutions can decide to apply a longer time for the conservation of the medical records. Regarding private health professionals, no time limit is required. However, the National Council for Physicians (CNOM) recommends to apply the same rules. The erasure of the medical record after the time limit is under the responsibility of the holders.

Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

10-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in France to include data from apps and devices in the EHR. In addition, the table displays how France have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records
There is an ICT system through which patients can access their EHR data
This is organised nationally. In France the DMP is open on a voluntary basis and contains all medical information the patient has consented to implement in it. The management of the DMP is organised through a website. It is filled in by medical professionals or the patient and also contains information from the National Health Insurance system. An Application for smartphones has also been developed in order for patients to have rapid access to their DMP.
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise,

sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	Health data from connected objects or apps cannot be automaticallly incorporated to the DMP (except if directly added by the patient) but presumably with the Espace Numérique de Santé through an offer of validated apps.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
France plans to join eHDSI for sharing summary records and ePrescriptions. Such services should be operational in 2021.	

Technical standards

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	
Policy level	• There are several national or regional policies to ensure use of standards for data interoperability
Policies are implemented on site for each healthcare/research institutions, however some standards are provided through an ongoing process with initiatives such as CASD; SNDS. Several standards are currently developed to support interoperability by various actors, e.g.: • Agence du Numérique en Santé (ANS) standards that are recommended for information systems for health care providers and institutions; • The standards proposed by the association Interop'Santé; • Those elaborated by the Region Occitanie which are aiming to propose solutions for health professionals, medical institutions and industries.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There are several national data security policies which address use of security standards in each healthcare provider sector (primary, secondary, tertiary, long term care)
Health data security is addressed by several bodies and institutions in France. The Agence du Numérique en Santé (ANS) elaborates an incitative policy with regards to security called General policy on the security of health information systems. This is rather a compilation of existing policies elaborated by several actors from the field of health. Following article L. 1461-1 PHC stating that "access to data is carried out under conditions that ensure the confidentiality and integrity of the data and the traceability of access and other processing, in accordance with a reference system defined by order of the ministers responsible for health, social security and digital technology, following the opinion of the CNIL", the SNDS has adopted specific rules for the security of the system.	
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	
Policy level	• There are several national data quality policies which address use of standards for each healthcare provider sector (primary, secondary, tertiary, long term care)
Several guidelines mentioned above include some criteria for the evaluation of the data quality. In addition, several references are listed through the ANS certification process used for those institutions that are hosting personal health data (ISO norms ISO 27001, ISO 20000, ISO 27018). Since Loi santé of 2016 the enhancement of the general quality and interoperability of information systems is an ongoing work. This is in particular relevant in the context of territorial Hospital groups as mentioned in Decree n°2016-524 (integrated into Art. R. 6132-15 PHC and following).	
Agencies which oversee the implementation of technical standards	
The supervision is usually done through the certification process for institutions hosting personal health data which is required by law. The Agence du Numérique en Santé (ANS) has elaborated with the relevant Ministries a referential for the needs of the certification process.	

10-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	Primary care data. https://www.snds.gouv.fr/SNDS/Accueil
Hospital and medical specialist care	Hospital and medical specialist care: https://www.snds.gouv.fr/SNDS/Accueil
Prescription drugs	Prescription drugs. https://www.snds.gouv.fr/SNDS/Accueil

11 COUNTRY FICHE CROATIA

The following sections provide an overview of the rules for processing of health data currently in place in Croatia both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[15]

11-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	**Health Data and Information Act** (Official Gazette 14/2019) determines the rights, obligations and responsibilities of legal and natural persons of the health system of the Republic of Croatia in the field of data management and information in health, defines the concepts and basic principles of collection, use and processing of health data and information, competent authorities, quality and processing of health data, their protection and inspection and professional supervision, for the purpose of comprehensive and effective use of health data and information in health care for the purpose of improving and preserving the health of the population in the Republic of Croatia. **Ordinance on the manner of keeping a personal health chart in electronic form** (Official Gazette 82/10) prescribes the manner of keeping a personal health record in electronic form. Medical data of the insured person in the e-Chart must be collected by the selected doctor of general practice/ family medicine, doctor of dental medicine, paediatrics specialist, gynaecology specialist, school medicine specialist (primary level of medical care). **Ordinance on the manner of keeping, storing, collecting and disposing of medical documentation of patients in the Central Health Information System of the Republic of Croatia** (Official Gazette 82/10) prescribes the manner of collecting and processing health data directly from patient in direct in person contact/care.
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	The following applies to the public healthcare sector: **Healthcare Act** (Official Gazette 100/2018) Article 38 (5) introduces the Health Communication Infrastructure, a network communication system that forms a common health basis for secure data exchange and interoperability tools (technical standards, classifications and network communication infrastructure). The purpose of the health communication infrastructure is to ensure the connectivity and interoperability of registers and information systems in the public health system of the Republic of Croatia and to provide common elements for interaction with citizens or other users.

[15] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Croatia. The authors of the report take full responsibility for any interpretations in the country fiche.

	The **Health Data and Information Act** provides that the legal obligation is basis for primary collecting and processing of any health data and information and the main purpose of the collection must be linked to a direct or indirect positive effect on personal and public healthcare interest. Secondary processing of health data is allowed for the purposes of archiving in the public interest, for the purposes of scientific or historical research or for statistical purposes for the purpose of studying and monitoring the health status of the population or for other purposes determined by applicable regulation. The **Ordinance on the manner of keeping a personal health chart in electronic form** prescribes the manner of keeping a personal health record in electronic form and further processing collected information according to legal obligation. The **Ordinance on the manner of keeping, storing, collecting and disposing of medical documentation of patients in the Central Health Information System of the Republic of Croatia** prescribes the manner of collecting and processing health data directly from patient in direct in person contact/care (primary level) in form of a personal health chart of the insured person which is submitted electronically to the central part of the integrated information system of CEZIH. Legally obligated public health institutions are processing personal data in public health interest.
Legal basis GDPR	• 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	**Healthcare Act**, Article 38 (5) as decribed above. **Health Data and Information Act** Section V sets out CEZIH: the Central Health Information System of the Republic of Croatia is the central system for storing health data and information for their standardized processing at the primary, secondary and tertiary levels of health care and is part of the health information infrastructure of the Republic of Croatia.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent
Specific legislation on **genetic testing**	
National legislation	Croatia has specific regulations for genetic testing. Genetic testing is mainly regulated by adopted EU Guidelines or National control plans (e.g. Quality assurance, NPPR). In addition: the following legislation applies: • **Act on Medically Assisted Insemination** (Official Gazette 86/2012) • **Act on the Application of Human Tissues and Cells** (Official Gazette 144/2012) • **Act on Human Organ Transplantation for Medical Purposes** (Official Gazette 144/2012) • **The Act on the Protection of Patients' Rights** (Official Gazette 169/04, 37/08)

11-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities

National legislation	**Health Data and Information Act** Section V sets out: • CEZIH which contains medical data collected for the purpose of providing patients' healthcare on primary, secondary and tertiary level; as well as • NAJS (National Public Health Information System) which contains medical data collected and stored in public health registries/ statistics (e.g. cancer, mortality, work injuries, occupational diseases, communicable and non- communicable diseases, health statistics, disability, psychosis and suicide, diabetes, drug abuse) The **Health Care Quality Act** (Official Gazette118/18) determines the principles and system of measures for achieving and improving the overall quality of health care in the Republic of Croatia and prescribes the procedure for accreditation of health care institutions, companies performing health care and private health care workers, as well as health technology assessment, all to ensure and reduce risk for the life and health of the patient.
Legal basis GDPR	• 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
Specific legislation addressing 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.	
National legislation	**Medicinal Products Act** (Official Gazette 76/13) is the act on the procedures for testing, placing on the market, manufacture, labelling, classification, distribution, pharmacovigilance, quality control, advertising, supply of the Croatian market with medicinal products and supervision of medicinal products, investigational medicinal products, active substances, and excipients. HALMED, The Agency for Medicinal Products and Medical Devices is the legal entity which public authorities **established** pursuant to the **Act on Medicinal Products and Medical Devices** (Official Gazette 121/03), supervised by the Ministry of Health.
Legal basis GDPR	• 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
Specific legislation addressing 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**	
National legislation	**Ordinance on the method for monitoring of deficiencies in medicinal products quality** (Official Gazette 113/08) **Ordinance on Essential Requirements, Classification, Registration of Manufacturers in the Register of Medical Device Manufacturers, Registration of Medical Devices in the Register of Medical Devices and Conformity Assessment of Medical Devices** (Official Gazette 84/13) regulates the procedure, method of registration and documentation for the registration of a manufacturer in the register of manufacturers. The procedure, method of registration and documentation for the registration of a Class I medical device in the register of medical devices are regulated by previous mentioned Ordinance. (Procedure for registration in the register and information on medical devices) **Ordinance on pharmacovigilance** (Offcial Gazette 83/13) regulates that all adverse reactions to medicinal products must be reported in writing to the Agency for Medicinal Products and Medical Devices (HALMED), and, in the case of vaccines, also to the Croatian Institute for Public Health (CIPH), according to the procedure set out in **Law on the implementation of Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in vitro diagnostic medical** (Official Gazette 100/18) and the **Ordinance on Pharmacovigilance**.
Legal basis GDPR	• 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

Specific legislation addressing 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**	
National legislation	The **Healthcare Act**, provides that • The Republic of Croatia shall provide public healthcare to its inhabitants through healthcare measures in a line with the healthcare plan. • WHO's International Health Regulations and EU Health Regulations are adopted and/or transposed into the legal system of the Republic of Croatia. The **Law on the Protection of the Population from Infectious Diseases** (Official Gazette 79/07, 113/08, 43/09, 130/17, 47/20) provides that • The Republic of Croatia shall provide prevention and protection measures from infectious/ communicable diseases • Coronavirus protection measures in a line with both previous mentioned Acts
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
No, it is not possible.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Croatia has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	According to the **Healthcare Act** the Croatian Institute of Public Health (CIPH) as central public health institute is collecting and analysing data and records in the field of epidemiology (e.g. HIV, flue, cancer, vaccines, diabetes, coronavirus), microbiology (e.g. TB, lung disease) health ecology (e.g. GMO, food and water safety) and managing as data controller other public health registries such as: mortality, mental diseases and disorders, occupational diseases, occupational injuries, disability, psychosis and suicide, health care for the elderly, drug addiction and abuse.
Legal basis GDPR	• 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
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • A healthcare professional may be given access to the data that he or she has submitted to the registry • 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 • Public sector researchers

* Note. 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.

11-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Croatia has specific legislation on this topic. Legal basis: • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
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.	Croatia has no specific legislation on this topic.
National legislation	Third- party public-sector researchers can use CEZIH medical data collected for the provision of healthcare, as well as NAJS medical data collected and stored in public health registries/ statistics (**Health Data and Information Act** section V).

11-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Croatia the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Croatia:	
Mechanism	• Application to a local research ethics committee • 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
There are no laws nor by-laws that regulate exemptions to the application to ethics committees. Some institutions require Ethics committee applications while some have their own access to health data protocols that do not require Ethics committee approvals in certain situations.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Croatia did not adopt such a system.	
Legislation has been adopted 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	
Croatia has specific legislation on this topic. Section IV of the National Health Data and Information Act regulates this.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Croatia has adopted a system to facilitate this. Nominally it has been regulated by the National Health Data and Information Act but in practice no systems have been adopted nor implemented.	
Legislation has been adopted which requires privately funded researchers to **share the research**	

data with public bodies
Croatia has no specific legislation on this topic.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
The use of data for secondary purposes, especially EHR-based data, is defined and operated mainly through contacts and access with the service provided / local EHR data custodian.

11-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Croatia.

Rights of the patient	How the right can be exercised in Croatia
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
The **Health Data and Information Act** Article 22 (2) states that the e-Chart is accessible only to authorized healthcare professionals who participate in treatment, health care and patient care, and those authorized persons to whom the patient has given explicit consent. The patient himself has an insight into the data in the e-Chart through the e-Citizens system upon request.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Croatia has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
There is no Croation legislation explicitly prescribing this issue, but the answer relates to the public health sector according to GDPR Article 17(3)(c) and (d); and due to the fact that all patients' medical records created in the public sector are part of multiple public registries, in which data is stored permanently. The private health sector might be different.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

11-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Croatia to include data from apps and devices in the EHR. In addition, the table displays how Croatia have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records
There is an ICT system through which patients can access their EHR data
This is organised nationally. The National Health Insurance Fund manages the national EHR portal which citizen's can access through the eCitizen portal. Although this is defined with the National Health Data and Information Act Article 22; this has yet not been fully operationally implemented.
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms

Mechanism	• Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Croatia participates in eHDSI through sharing summary records and prescriptions. In Croatia, doctors can access health data of citizens coming from Czech Republic since September 2019 and from Malta since 24 Feb. 2020. Medicines can be retrieved in Croatian pharmacies with an ePrescription from Finland since January 2019).	
Technical standards	
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	
Policy level	• 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)
Interopeability policy is defined in very general terms in the National Health Data and Information Act, Article 4 'basic prinicples for the collection, use and processing of health data and information'.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
Again, it is described generally, without defining or naming data security standards in the National Health Data and Information Act under section V 'Health data and information protection'.	
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	
Policy level	• There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
Again, it is described generally, without defining or naming exact technical data quality policies in the National Health Data and Information Act under section IV 'Quality and processing of data and health information'.	
Agencies which oversee the implementation of technical standards	
The **National Health Data and Information Act** defines the Ministry of Health as an institution that should oversee the implementation of such standards and adherence to this, and other applicable, Acts.	

11-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	Croatian Institute of Public Health (HZJZ) https://www.hzjz.hr/en/
Hospital and medical specialist care	Croatian Health Insurance Fund (HZZO) www.hzzo.hr
Prescription drugs	The Agency for Medicinal Products and Medical Devices of Croatia (HALMED) http://www.halmed.hr/ Croatian Health Insurance Fund (HZZO)

12 COUNTRY FICHE ITALY

The following sections provide an overview of the rules for processing of health data currently in place in Italy both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[16]

12-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The main sector-specific legislations that currently regulate the processing of health data for direct care in the country are the following: • Legislative Decree n. 196 of 30 June 2003 (**Data Protection Code**) as amended by Legislative Decree n. 101 of 10 August 2018 which harmonized the Data Protection Code to the GDPR. o Articles 2-sexies transposes Article 9(2)(g) GDPR. o Article 2-septies provides that the processing of genetic, biometric, and health data should occur in compliance with specific ***safeguards measures*** to be outlined within a specific provision by the Italian DPA. At the time of writing, the DPA has yet to issue this provision. o *Title V* regarding the "*Processing of personal data in the health domain"* and comprising Articles 75-93, concerns general principles underpinning health data processing, the ways to inform data subjects and to provide the privacy notice, the way to deal with prescriptions, medical records, and the certificate of childbirth assistance. • Provision n. 55 of 7 March 2019 (**Provision 55/2019**) provided by the DPA further clarifies that, in addition to the above, the following legal bases can be used for the processing of health-related data: i) *reasons of public interest in the field of public health* and ii) *reasons of preventive medicine, diagnosis, health or social care or therapy or the management of health or social systems and services* • Article 12 of Law Decree n. 179 of 18 October 2012, converted into law n. 221 of 17 December 2012, as subsequently amended (**D.l. 179/2012**) and the Decree of the President of the Council of Ministers (DPCM) n. 178 of 29 September 2015, "Regulation of Electronic Health Records" (**DPCM 178/2015**). D.l. 179/2012 is the national legislation establishing the Electronic Health Record (EHR) "*Fascicolo Sanitario Elettronico*" (henceforth: **FSE**), whose rules of functioning are further specified in DPCM 178/2015. The functioning of the FSE is based on consent (though Provision 55/2019 amended this in light of the GDPR. • Against the backdrop of the COVID-19 pandemic, the Italian Government has issued Law Decree n. 34 of 19 May 2020 (**D.l 34/2020)**, coordinated with the conversion law July 17, 2020, n. 77, which, in Article 11, introduces a number of changes regarding the functioning of the FSE, including the abrogation of art. 3bis, which required consent for feeding the FSE. • **Guidelines 4/6/2015** of the DPA relates to "*dossier sanitario*". It is an EHR that differs from the FSE in the fact that the accessible data are generated by a single data controller and not by several health facilities as autonomous data controllers,

[16] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Italy. The authors of the report take full responsibility for any interpretations in the country fiche.

	as it is the case with the FSE. The processing is based on consent. Technical aspects that impinge on the functioning of EHRs are: • Legislative Decree n. 82 of 7 March 2005 (**Digital Adminstration Code**), specifically Article 64 and 73. • **Circular n.3 of 2 September 2019** of AgID ("Agenzia per l'Italia Digitale"), which regulates the procedure for national access to the FSE, and additional functionalities that the National Infrastructure for Interoperability (INI) makes available to the Regions to ensure interoperability among regional FSE systems.
Legal basis GDPR	• 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 • Other combination: 6(1)(e) public interest + 9(2)(g) substantial public interest on the basis of Union or Member State law
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	**D.l. 179/2012 art. 12** and **DPCM 178/2015** The EHR systems in Italy facilitate data sharing and portability for healthcare provision purposes, notably when it comes to the FSE which is constructed *ab initio* as portable personal health information: • ***Fascicolo sanitario elettronico*** (FSE): the whole set of health data and documents related to present and past clinical events regarding an individual citizen ("assisted person"); it can be accessed by every national healthcare system-accredited provider or professional for the purpose of care. • ***Dossier sanitario***: it differs from the FSE in that the health documents and information accessible via this tool are generated by multiple professionals within a single healthcare provider (data controller), and not by several data controllers as it is the case for FSE. • ***Cartella clinica (digitale)***: it collects all data relating to a patient's recovery for a single case of hospitalization. Healthcare professionals and providers are allowed to share data only on the basis of patient consent, except in cases of extreme urgency (pursuant to Art. 14 of DPCM 178/2015).
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Italy has no specific legislation on this topic. In Italy, to date, national and/or regional laws and regulations on mHealth/digital health are lacking. Tools such as medical apps may be used by health professionals on the basis of other existing legislation (in particular, see Provision 55/2019 of the DPA). On 10 July 2012, however, the Ministry of Health has issued "**National Guidelines on Telemedicine**", which have been followed, in March 2017, by **DPCM 12/1/2017**: **"**Definition and updating of essential levels of care" that provided for the reimbursement of "alternative communication software" and "alarm and tele-assistance devices", particularly for disabled patients. The Guidelines were adopted before amendments to the Data Protection Code of 2018 and therefore use terminology that is not always updated.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(h) health or social care
Specific legislation on **genetic testing**	
National legislation	Italy has specific regulations for genetic testing. • **Agreement 15/7/2004** of the State-Regions Conference: "Guidelines for medical genetics activities" • **Agreement 26/11/2009** of the State-Regions Conference is geared to foster the implementation of the aforementioned Guidelines for medical genetics activities. • **Agreement 13/3/2013** of the State-Regions Conference: "Guidelines on

	genomics in public healthcare" • **DPCM 12/1/2017** "Definition and updating of essential levels of care" • **Agreement 26/10/2017** of the State-Regions Conference: "Plan for innovation in the healthcare system based on omics sciences" • **Provision 146/2019** issued by the DPA contains provisions regarding the processing of genetic data

12-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	**Provision 55/2019** of the DPA provides a clarification on the rules for the processing of health-related data in the health sector, and the relevant legal bases that apply for the re-use of health data for planning, management, administration and improvement of the health and care systems. **D.l. 179/2012**: Article 12 paragraph 2 provides that the FSE EHR is established for the purpose of: (i) prevention, diagnosis, care and rehabilitation; (ii) investigation and scientific research in the medical, biomedical and epidemiological domains; and (iii) healthcare planning, evaluation of the quality of care and healthcare provision **DPCM 178/2015**: Articles 18-20 concern the "processing for management purposes" and regulate in detail who can process data and how data can be processed for planning, management, administration and improvement of the health and care systems. **DPCM 3/3/2017**: Art. 3.4 endows the Ministry of Health with the prerogative to process disease registries' data for purposes related to the management of the healthcare system.
Legal basis GDPR	• Other combination: 6(1)(e) public interest + 9(2)(g) substantial public interest on the basis of Union or Member State law
Specific legislation addressing 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.	
National legislation	Besides EU legislation (the imminently applicable Reg (EU) 536/2014, and Regulation (EU) 745/2017), the relevant legislation in this regard is the Italian Privacy Code, art. 2-sexies paragraph 2 letter z, which provides that the processing of special categories of personal data for the purpose of market approval of medicines and devices can occur on the basis of relevant public interest.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	Besides the applicable Reg. (EU) 1235/2010, the relevant national legislation concerning pharmacovigilance is the Health Ministry Decree of 30 April 2015, which transposed within Italian legislation Directives 2010/84/EU and 2012/26/EU. However, this law does not specifically address data protection aspects related to

	pharmacovigilance activities. The only reference to pharmacovigilance can be found in the **Italian Privacy Code**, **art. 2-sexies paragraph 2 letter z**, which provides that pharmacovigilance activities that involves the processing of special categories of personal data can be pursued on the basis of relevant public interest.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	**Ministerial Decree of 15 December 1990** (Information System for Infectious and Diffusive Diseases) establishes five classes of notification, which meets criteria of epidemiological relevance and differentiated needs for prophylaxis. The data is received by the General Directorate of Prevention and the reporting of these diseases is mandatory. In addition, depending on the class of notification, the timing, notification methods and flows of the disease itself change. SIMID, Information System for Infectious and Diffusive Diseases, is the information system used, aimed at managing the database of infectious diseases. The information flow is carried out through the doctor, hospital or primary care physician, who diagnoses the infectious disease and reports it to the competent Local Health Authority, the Local Health Authorities in charge of adopting any prophylactic measures to protect public health, the Region (Public Health Agency) with supervision and coordination action, the Central Bodies (Ministry of Health, ISTAT, Istituto Superiore di Sanità) and possibly international ones (EU, WHO). In addition, the provisions of the Italian Data Protection Codes apply.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
In Italy, the COVID-19 surveillance has been shaped, first, by **Health Ministry, Circular n.1997 of 22 January 2020**, which contained the first criteria and modalities for reporting cases of SARS-CoV-2 infection. Afterwards, a number of other Circulars with integrations and updates were provided. On February 27, 2020, the Civil Protection, through the **Ordinance n. 640**, has entrusted the epidemiological and microbiological surveillance for COVID-19 to the Istituto Superiore di Sanità (ISS). At present, all Regions and Autonomous Provinces forward daily data to the ISS for all individuals with SARS-CoV-2 infection confirmed in the laboratory. The Department of Infectious Diseases of the ISS processes and analyzes the data of the platform and makes them available to allow the analysis of the epidemic throughout the country.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• To our knowledge, Italy has no specific legislation on this topic.
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	The relevant legislations with regard to "surveillance systems and [disease] registries" are DPCM 3/3/2017 and **L. 29/2019**. Art. 3.4 DCPM 3/3/2017 identifies the Ministry of Health as data controller for surveillance systems and registries of national and regional relevance, which are listed in Annex A of the DPCM. Art. 3.5 identifies other national public agencies as data controllers for specific registries, and can access and process the data collected in that specific register for the purposes of research and care. L. 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.

Legal basis GDPR	• 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 • Other combination: 6(1)(e) public interest + 9(2)(j) scientific research
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • National governmental agencies • Patient organisations • Public sector researchers • Private sector organisations

* Note. 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.

12-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Italy has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes • Other: Art. 110-bis.4 of the Data Protection Code (for IRCCS; research hospitals accredited with the MoH)
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.	Italy has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes
National legislation	In Italy, the legislation does not differentiate between not for profit researchers and for profit researchers. The Italian Data Protection Code encompasses a specific section devoted to scientific research ("*Title VII – Processing for archiving purposes in the public interest, scientific or historical research or for statistical purposes*"), and, within this section, two articles that specifically relate to data processing for medical, biomedical and epidemiological research purposes (namely, arts. 110 and 110-bis). The re-use of data by third party researchers, either public or private, is regulated in Art. 110-bis of the Data Protection Code. The DPA may authorize the processing either on an *ad hoc* basis upon request by the data controller (paragraph 2), or by means of general provisions (paragraph 3), through which the DPA gives *prior* general authorization to specific kinds of data controllers and processing activities, while also outlining the safeguards to be adopted.

12-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Italy the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Italy:	
Mechanism	• 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 • Other: It is worth noting that proposals have been made to establish a centralized data governance and access body in the context of Italian research hospitals. At the time of writing, however, this board akin to a national Data Access Committee (DAC) has yet to be implemented.
Access to health data for research purposes in Italy (other than those pertaining to disease registries and surveillance systems) presently lacks a harmonized framework. The most common way to access health data is by means of research collaborations, whereby research groups interested in getting access to data engage directly with the data controller that has collected such data. In most cases, access to the data requires engagement with an ethics committee, whereby the data controllers must obtain (or must have obtained) ethics approval for transferring data to third party researchers. In practice, however, in some cases (especially for basic research where no IP issues are involved), the transfer of data happens without engagement with an ethics committee.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Italy did not adopt such a system.	
Legislation has been adopted 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	
Italy has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Italy has adopted a system to facilitate this. Accredited Italian research hospitals (IRCCS, the Istituti di Ricovero e Cura a Carattere Scientifico) can re-use health data for research purposes. Italian Data Protection Code, paragraph 4 of art. 110-bis states that "the processing for scientific research purposes of personal data collected for clinical activity by research hospitals ("Istituti di ricovero e cura a carattere scientifico") does not constitute further treatment by third parties, due to the instrumental nature of the activity of health care provided by the aforementioned institutions with respect to research, in compliance with the provisions of article 89 of the Regulation". At the time of writing, a request for clarification regarding the scope of interpretation of Art. 110-bis, paragraph 4 has been submitted by the ACC-GDPR Committee and is still pending with the Italian DPA.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
No, other than e.g. private research hospitals accredited with the MoH (private IRCCS), which are required to provide data for e.g. the purpose of government of the healthcare system.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
Italy presently lacks a single entry point for data re-use for healthcare management and scientific research purposes. In the country, there are at the same time several systems to share data for secondary use: one national system, several specific regional systems, and several sector specific systems. (i) For health data within the national FSE system, the Ministry of Health and/or the Ministry of Labor are data controllers. Accordingly, they provide access to such data. (ii) For health data of which individual regions are data controllers (e.g. data collected within regional FSE systems), Italian regions have established their own system and regional regulations for transferring such data and processing requests of access (e.g. by researchers). There are no	

web portals on which researchers across the country or Europe can request access to data. Accordingly, access to such data seems to hinge on inside knowledge of the system by local researchers.

(ii) For health data contained within the national network of tumor registries and surveillance systems, access is provided by the Ministry of Health, upon consultation with the DPA. Again, there is no web portal on which researchers across Europe can request access to data.

In addition, it should be noted that efforts at harmonizing data access procedures for secondary use of health data for scientific research are also being carried out by research networks ("*reti di ricerca*") accredited with the Italian Ministry of Health, such as the oncologic (Alliance Against Cancer) and cardiologic networks. These are in the process of negotiating the establishment of single points of entry for access to health data collected, processed and stored by affiliated institutions (which for the most part are IRCCS)

12-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Italy.

Rights of the patient	How the right can be exercised in Italy
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Italy has not adopted specific legislation on the application of such a right in the area of health.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Italy has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
D.l 179/2012 and DPCM 178/2015 allows individuals to obscure records in their FSE. Data rendered obscure cannot be accessed by healthcare providers and professionals, apart from those who have generated such data. This, however, does not amount to have the records deleted.	
Article 20 'right to data portability'	• Through a formal regional data portability request system established by legislation

12-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Italy to include data from apps and devices in the EHR. In addition, the table displays how Italy have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records
There is an ICT system through which patients can access their EHR data
• This is organised nationally. • This is organised regionally. Regions have individually established their IT system and access portal for the FSE. Citizens can access their FSEs in the portal of their own region through different authentication methods. In the event of change of residency (move to another region), the regional portal for access to the FSE will change as well. In addition, Ministerial Decree of 25/10/2018 introduced the possibility for citizens to access their FSEs also through a single national system using a national portal. Using the new portal, the access point is unique throughout Italy, and the patient can access his/her FSE using the authentication methods defined at the national level. Circular n.3 of 2 September 2019, has been issued by AGID to regulate (i) the procedure for

national access to the FSE also through the national portal and(i i) the additional functionalities that INI makes available to the Regions, necessary to ensure the operability of the system.

Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms

Mechanism	It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs. In case apps and devices are used outside of medical care, healthcare providers cannot incorporate them into the FSE. On the contrary, if apps, devices, sensors, etc., are used as part of medical treatments provided by healthcare professionals, they can be fed into the FSE.

Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'

by 2021 both services (ePrescription and Patient Summary) will be gradually implemented in Italy.

Technical standards

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

Policy level	• 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)

In Italy, the healthcare system is organized regionally (19 regions and 2 autonomous provinces). Against this fragmented landscape, there is one national interoperability policy, that ensures that the FSE systems implemented at the regional level can be interoperable. In addition, the national standards are also in line with EU standards, to ensure interoperability at the European level.

Specifically, the national architecture for the FSE is based on a distributed model. Each Region has implemented a platform with two main components: 1) one or more repositories to store digital health documents; and 2) an index register, which contains a set of metadata describing the documents (including pointers to the repositories where these documents are stored).

In particular, in order to support patient mobility throughout the country, the documents are always stored in the repository relating to the facility that produced them, while the metadata are stored in the index register of the patient's care region. For this reason, regional FSE platforms should be able to interoperate with each other. This is also achieved through a national infrastructure (called INI), which acts as a broker with respect to the various platforms.

The entire national interoperability architecture is based on an **Italian localization of the IHE XDS international standard**; the communication protocols (e.g. to search and retrieve documents or to transmit metadata from one region to another) are aligned to this standard. With reference to the structuring of clinical documents, instead, the **reference standard is HL7 CDA Rel. 2.0**. In particular, several national implementation guides have been defined (with the involvement of HL7 Italia). They describe how to use this standard to structure the various types of documents (reports, prescriptions, synthetic health profile, discharge letters, etc.).

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

Requests for access to national interoperability services may only be made by authorized users. In this respect, a number of roles have been specified, in accordance with the regulations in force, which profile the different users (e.g. general practitioners, specialist doctors, patients, etc.). After a **strong type of authentication** (**SPID level 2, TS-CNS or username and password + OTP**), for each request a statement adhering to the **OASIS SAML 2.0 standard** is generated by the regional node. This assertion is a computer document that contains a series of attributes: in addition to the role of the user (verified by the regional domain), the reason for the request, the social security number ("*codice fiscale*"), etc.. This assertion is used by the access control components to verify whether or not the user has access rights to the requested service.

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

Policy level	• There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

The information contained in clinical documents in HL7 CDA Rel. 2.0 format (including narrative information) must be appropriately coded in order to avoid ambiguities and facilitate semantic interoperability. In this regard, the current legislation has established four coding/classification systems: **LOINC**, to encode laboratory observations; **ICD9-CM**, to classify diseases; **AIC** and **ATC** for drug coding.

Agencies which oversee the implementation of technical standards

The agency that currently oversees the implementation of such standards policies is AgID (Agency for Digital Italy). Experts from the Italian National Research Council, among others, have been involved in the standard-setting procedures, by being involved in discussions with policymakers, and by actively designing the FSE infrastructure.

13 COUNTRY FICHE CYPRUS

The following sections provide an overview of the rules for processing of health data currently in place in Cyprus both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[17]
Please note that currently the health system of Cyprus is under major reform and health data processing regulations are being drafted in a new law. Therefore, many details are not yet clarified.

13-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	Details of legislation are not available yet.
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	With the implementation of the first phase of the general health system of the country the primary care doctors received a quite basic EHR system. The benefitiary provide consent for that to be used. Other doctors can access that data if you are reffered to them.
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Cyprus has no specific legislation on this topic. A new law, Law 59(I)/2019 which shall provide for electronic health, is currently under consideration (the only authority to govern eHealth has recently been established). This law will regulate the provision of digital health services.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	Cyprus does not have specific regulations for genetic testing.

[17] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Cyprus. The authors of the report take full responsibility for any interpretations in the country fiche.

13-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Cyprus has no specific legislation on this topic.
Specific legislation addressing 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.	
National legislation	Cyprus has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Cyprus has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Cyprus has no specific legislation on this topic.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Cyprus has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	Cyprus has not adopted specific legislation on this topic.

* Note. 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.

13-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Cyprus has no specific legislation on this topic.
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.	Cyprus has no specific legislation on this topic.

13-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Cyprus the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Cyprus:	
Mechanism	• Application to a local/national research ethics committee and the DPA • Other: Research application to the Ministry of Health
Even if pseudonymised the National Bioethics Committee needs to inform the researcher whether there is a need for full application for ethics. There is an application for this and a cost of 50EUR. The Ministry of Health needs approval that an ethics is needed or not, from that committee to be attached at the application for research.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Cyprus did not adopt such a system. However, a new law, Law 59 (I)/2019 which shall provide for electronic health, is currently under consideration and will manage health data. The law should include an article on data altruism.	
Legislation has been adopted 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	
Cyprus has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Cyprus did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Cyprus has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
Data cannot be provided for research unless an application is submitted to the Ministry of Health, the Bioethics committee and the Personal Data Protection Ombudsman.	

13-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Cyprus.

Rights of the patient	How the right can be exercised in Cyprus
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Cyprus has not adopted specific legislation on the application of such a right in the area of health.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Cyprus has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions
A law is currently being drafted and there will be a provision for this right.	
Article 20 'right to data portability'	• Through a formal national data portability request system established by legislation

13-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Cyprus to include data from apps and devices in the EHR. In addition, the table displays how Cyprus have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. In theory, with the oprimary care information system benefitiaries have the benefit of accessing their health records.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so As the law is currently being drafted it is not sure yet whether there will be such an obligation.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Cyprus does not yet participate in eHDSI but plans to do so by 2025.	
Technical standards	
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	
Policy level	• 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)
With the full implementation of the healthcare system all healthcare providers that join the general	

health system will have to use the existing system. No interoperability issues arise as all providing members of the Health Insurance Organisation (HIO) thus use the same system. However, those who not belong to HIO cannot access health records created by HIO providers.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There are no national or regional data security policies to ensure use of standards for data security
Currently there is a law being drafted that will encompass all policies to secure data security. Therefore, in the future there will be one national data security policy which addresses the use of security standards across all healthcare provider sectors.	
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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.
Agencies which oversee the implementation of technical standards	
The eHealth agency oversees the implementation of technical standards.	

14 COUNTRY FICHE LATVIA

The following sections provide an overview of the rules for processing of health data currently in place in Latvia both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[18]

14-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	**Law On the Rights of Patients** [Pacientu tiesību likums], Latvijas Vēstnesis, 205, 30.12.2009.[19] Of particular relevance are the following provisions: • Section 9 regulates the right to become acquainted with medical documents in relation to medical care that the patient receives/has received. • Section 4.6 regulates a patient's right inter alia to receive information regarding the medical services provided to him or her and the justification for the termination of medical treatment, as well as the results of diagnostic examinations and functional assessments (extracts, true copies and copies) • Section 10 regulates the protection of a patient's data. It includes a general clause in Section 10.1 that "Information, which relates to an identified or identifiable patient, shall be protected in accordance with the laws and regulations governing the protection of the data of natural persons." • Section 10.6 regulates the right of a representative of a minor to receive information about a minor patient. This section is ambiguous regarding the exact situations when information can be withheld from the legal representatives (Section 10.6 indicates Section 13, but Section 13 regulates consent to medical care) and has been criticized in doctrine.[20] Rules regarding medical documents, including their content are set forth in Cabinet Regulation No. 265 of 4 April 2006, **Procedures for Keeping Medical Documents** [Medicīnisko dokumentu lietvedības kārtība], Latvijas Vēstnesis, 57, 07.04.2006. **Medical Treatment Law** [Ārstniecības likums], Latvijas Vēstnesis, 167/168, 01.07.1997. Chapter XIV sets forth key requirements regarding the Health Information System. What concerns electronic keeping of the records, they are regulated in detail with the Cabinet Regulation No. 134 of 11 March 2014 **Regulations Regarding the Unified Electronic Information System of the Health Sector** [Noteikumi par vienoto veselības nozares elektronisko informācijas sistēmu], Latvijas Vēstnesis, 52, 13.03.2014. **Personal Data Processing Law** [Fizisko personu datu apstrādes likums], Latvijas Vēstnesis, 132, 04.07.2018, Section 25 Paragraph 2 addresses operationalization of Articles 9.2 and 9.4 GDPR.

[18] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Latvia. The authors of the report take full responsibility for any interpretations in the country fiche.

[19] https://likumi.lv/ta/en/en/id/203008-law-on-the-rights-of-patients please note that the official English translation is outdated. Please consult the Latvian version instead: https://likumi.lv/ta/id/203008-pacientu-tiesibu-likums

[20] See Agnese Gusarova, 10.pants. Pacienta datu aizsardzība, pp.166-197. In Santa Slokenberga ed. Pacientu tiesību likuma komentāri (Latvijas Vēstnesis 2019).

Legal basis GDPR	This is not comprehensively regulated at the national level. The following can be argued based on how the national law is framed. • 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 • Other combination: o As the national law is framed, a clear-cut distinction between 6.1.c and 6.1.e cannot be easily drawn. The answer will depend on several considerations, including the status of the healthcare provider in question. o As this question is not expressis verbis nationally regulated, it cannot be entirely excluded that there is a healthcare provider that mandates consent, and therefore Art. 6(1)(a) Consent and 9(2)(a) Consent apply. That, however, is not required by law. o In addition to what has been marked, it cannot be excluded that healthcare that is privately funded triggers another combination; e.g.Art.6(1)(b) and 9(2)(h). Contracts for such healthcare fall in the domain of civil (private law). On the other hand, if 'national law' under Art.6(3)(b) GDPR covers general clauses such as a right to medical care, then Art.6(1)(b) and 9(2)(h) could be less often used.
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	This is not comprehensively regulated at the national level. However, several provisions are relevant to this question. For example: In accordance with Section 8 of the Law On the Rights of Patients, a patient has the right to choose a health care provider and professional. Taking into account the below mentioned (see "other"), the health care provider and professional involved in the patients' health care provision may share the patients' personal data if the patient has agreed to the involvement of another medical practitioner in the provision of health care services. In accordance with Section 10, Paragraph 5, Clause 1 of the Law on the Rights of Patients, upon a written request and receipt of a written permission of the head of the medical treatment institution, information regarding the patient shall be provided (not later than five working days after receipt of the request) to medical treatment institutions - for the purpose of achieving the objectives of the medical treatment. In accordance with Section 79 of the Medical Treatment Law and Paragraph 4 Clause 1 of the Regulations regading the Unified Electronic Information System of the Health Sector, the information accumulated in the health information system regarding patients shall be provided for the achievement of medical treatment objectives (this is as a general statement).
Legal basis GDPR	• 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 care • Other: - This issue is not particularly regulated. It derives from the overall framework in how different processes are organized, as well as when they are not specifically organized, direct application of GDPR rules. Therefore, other options GDPR allows for could also be possible. - Access rights are expressis verbis regulated under Section 10 Paragraph 5 Clause 1 of the Law On the Rights of Patients, but it is not the only avenue that enables data sharing. - As the national law is framed, a clear-cut distinction between 6(1)(c) and 6(1)(e) cannot be easily drawn. In some cases, legal obligation will apply. In others one can also discuss relevance of the public interest clause.
Specific law addressing the processing of health data **for providing digital health services**	

National legislation	Latvia has no specific legislation on this topic. Digital health services are not specifically regulated, and neither is data processing in regard to digital health services. In Latvia, digital health services are defined as telemedicine in accordance with Medical Treatment Law, Section 1, Paragraph 29. Section 6 of Law on Pracice Doctors (unofficial translation) contains a prohibition that in some situations can be relevant to the provision of digital health services. Par prakses ārstiem, Latvijas Vēstnesis, 113, 08.05.1997. Lawfulness of this provision can be questioned.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	Other: Even though medical devices (including the use of health-related softwares) could be prescribed, see Cabinet Regulation No. 175 of 8 March 2005 **Regulations Regarding Manufacture and Storage of Prescription Forms**, as well as **Writing out and Storage of Prescriptions** [Recepšu veidlapu izgatavošanas un uzglabāšanas, kā arī recepšu izrakstīšanas un uzglabāšanas noteikumi], Latvijas Vēstnesis, 48, 23.03.2005, the question of prescription of such medical devices is not specifically regulated. It cannot be excluded that prescriptions take place and such data are used. Likewise, when a recipe is not required, a doctor may nonetheless suggest using such an app. It could be argued that the same legal grounds that relate to the provision of medical care could also apply to the use of data, however, because of the uncertainty in Latvia (regulation lacks), one could also argue that consent is the most relevant legal basis.
Specific legislation on **genetic testing**	
National legislation	Latvia does not have specific regulations for genetic testing. General requirements that apply to laboratories need to be met; genetic testing can be carried out in accordance with such medical technology that is approved. See Section 8.5 of **Human Genome Research Law** [Cilvēka genoma izpētes likums], Latvijas Vēstnesis, 99, 03.07.2002. Approved methods can be seen here.

14-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Section 10, Paragraph 5[1] of the Law On the Rights of Patients lists those actors who have right to receive patient data in accordance with the procedures laid down in the laws and regulations regulating the field of health care. The paragraph also sets forth those actors who have right to process information accumulated in the health information system regarding a patient in accordance with the procedures and in the amount laid down in the laws and regulations regarding the data to be processed in the health information system.[21] As the legal framework is fragmented, below only illustrative examples are provided of

[21] Key rules that regulate the health information system are set forth in Chapter XIV of Medical Treatment Law; further details are set forth in the Regulations Regarding the Unified Electronic Information System of the Health Sector.

	laws relevant to the planning, management, administration and improvement of the health and care systems relevant to tasks carried out by the National Health Service (NHS, in Latvian: Nacionālais veselības dienests). NHS is key state authority, which is responsible for planning, management, administration and improvement of the health and care systems in Latvia. NHS is responsible for the national information systems containing personal data regarding health: • The database of the recipients of health care services (state funded); the system is set up in accordance with the **Health Care Financing Law** [Veselības aprūpes finansēšanas likums], Latvijas Vēstnesis, 259, 31.12.2017 (Section 13, par. 2) • The health care services payment settlement system "Management Information System" is mentioned in the Cabinet Regulation No.850 of **By-laws of the National Health Service** (unofficial translation) [Nacionālā veselības dienesta nolikums] Latvijas Vēstnesis, 178, 10.11.2011. The regulation defines the competence (functions, tasks and rights) of the NHS; the system cannot be considered to be based on the law; nevertheless, this system contains information about persons, medical personnel and patient's medical information (personal data); the system is for planning, management, administration purposes; • The Unified Electronic Information System of the Health Sector; set up in accordance with the Regulations Regarding the Unified Electronic Information System of the Health Sector which specifies what kind of information should be included in this System; this Regulations determines centralised processing of the data related to a person's health (specified in this Regulation) that is needed for medical treatment (including, electronic prescriptions in circulation between a medical practitioner and pharmacist; referrals for receipt of a health care service).
Legal basis GDPR	• 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 • Other: Key authority in planning, management, administration and improvement of the health and care system is the National Health Service, even though the Ministry of Health retains the overarching legal and political respolsibility of the field. However, several other authorities could also be involved, e.g. the Centre for Disease Prevention and Control that focuses on matters relating specifically to epidemiological safety or Health Inspectorate that carries out supervisory functions in the field (e.g. quality of medical care). It is difficult to draw a distinction between legal obligation and public interest under Art.6 in these cases; however, as the national law is phrased the legal obligation is the likeliest option. Likewise, it cannot be precluded that in some cases public interest in the field of public health could be relevant, but in others – healthcare under Article 9. It is unlikely that other combinations or legitimate interest claim could be relevant.
Specific legislation addressing 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.	
National legislation	Latvia has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	The competent authority (the State Agency of Medicines) has been given a right to access patient data for pharmacovigilance purposes, see Section 10, 5^1 clause 3 of the Law On the Rights of Patients. **By-laws of the State Agency of Medicines** (unofficial translation) [Zāļu valsts aģnetūras nolikums] Latvijas Vēstnesis, 123, 07.08.2012, assign competence to the authority in these matters, see Paragraph 4 Clause 2. Cabinet Regulation No. 47 of 22 January 2013 **Pharmacovigilance Procedures** [Farmakovigilances kārtība] Latvijas Vēstnesis, 22, 31.01.2013 prescribes the procedures for pharmacovigilance. In order to ensure effective functioning of the pharmacovigilance system, a medical practitioner or a pharmacist shall report on the observed suspected adverse drug reactions to the State Agency of Medicines or the

	respective marketing authorisation holder; a patient has the right to report to the State Agency of Medicines or the marketing authorisation holder on the suspected adverse drug reactions. This reporting procedure includes detailed information about a patient. Cabinet Regulation No. 689 of 28 November 2017 **Procedures for Registration, Conformity Assessment, Distribution, Operation and Technical Supervision of Medical Devices** (unofficial translation) [Medicīnisko ierīču reģistrācijas, atbilstības novērtēšanas, izplatīšanas, ekspluatācijas un tehniskās uzraudzības kārtība] Latvijas Vēstnesis, 22, 31.01.2013 addresses monitoring of medical device safety (see Chapter 12). Annex 25 to these Regulations is filled out by a patient and includes the patient's data, See Paragraph 191, Clause 1.
Legal basis GDPR	• 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 • Note: Legal obligation is the likeliest base. It cannot be exclude that one might also wish to argue for public interest. Because of how national law is phrased, a clear line between 9.2.h and 9.2.i cannot be drawn.
Specific legislation addressing 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**	
National legislation	Section 12, Paragraph 2 of **Epidemiological Safety Law** [Epidemioloģiskās drošības likums], Latvijas Vēstnesis, 342/345 enables the provision of official information, also to the World Health Organisation and the institutions of the European Union, regarding the epidemiological situation in Latvia shall be prepared by the Ministry of Health or another authority authorised thereof. However, it is highly doubtful this can be used as basis for the processing of patient data. Instead, the access right of the Centre for Disease Prevention and Control set forth in the Law On the Rights of Patients might need to be invoked. To what extent this would be possible, is uncertain. See Section 10, Paragraph 5^1, Clause1 of the Law On the Rights of Patients.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible to some degree. It is possible at the national level based on Section 10 Paragrap 5^1 Clause 1 of the Law On the Rights of Patients and Paragraph 3, Clauses 3 and 4, as well as Paragraph 4 Clause 2 and Paragraph 5 Clause 1 of Cabinet Regulation No. 241 of 3 April 2012 **By- laws of the Centre for Disease Prevention and Control** [Slimību profilakses un kontroles centra nolikums] Latvijas Vēstnesis, 55, 05.04.2012. It is ambiguous regardig data transmission to ECDC.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Latvia has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	Please note that the national legal framework regarding disease registries is fragmented and ambiguous. See Regulations Regarding the Unified Electronic Information System of the Health Sector. Cabinet Regulation No. 746 of 15 September 2008 **Procedures for Establishing, Supplementing and Maintaining a Register of Patients Suffering from Certain Diseases** [Ar noteiktām slimībām slimojošu pacientu reģistra izveides, papildināšanas un uzturēšanas kārtība], Latvijas Vēstnesis, 146, 19.09.2008. Some other registries are set forth in accordance with **Sexual and Reproductive Health Law** [Seksuālās un reproduktīvās veselības likums], Latvijas Vēstnesis, 27, 19.02.2002.
Legal basis	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health

GDPR	• 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 • Other: A clear-cut line between legal obligation and public interest is difficult to draw in Latvia. Likewise, either public interest or healthcare could be relevant, depending on circumstances.
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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. • Other national governmental agencies

* Note. 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.

14-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Latvia has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
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.	Latvia has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
National legislation	In Latvia, the legislation does not differentiate between not for profit researchers and for profit researchers. Section 10, Paragraphs 7-9 set forth rules regarding the use of patient data that are part of medical documentation in scientific research. See Law On the Rights of Patients. Paragraph 7 sets out that research that is based on consent of the patient (data subject) or research that processes information that that does not allow to (directly or indirectly) identifying the patient does not need a specific authorisation. However, other research situations need to be approved. Requirement for the approved is set forth in Paragraph 8. Detailed rules are outlined in the Cabinet Regulation No. 446 of 4 August 2015, **Procedures for Using the Patient Data in a Specific Research**, Latvijas Vēstnesis, 152, 06.08.2015, which is issued pursuant to Section 10, Paragraph 8, Clause 2 of the Law On the Rights of Patients. What concerns statistics specifically, it is separately regulated. Official statistics is

	regulated under the **Statistics Law** [Statistikas likums], Latvijas Vēstnesis, 118, 18.06.2015.[22] The legal framework for statistics in the area of health is fragmented. E.g. requirements regarding specific forms for the collection of data are regulated by the Cabinet. [23] The Centre for Disease Prevention and Control has competence to acquire, compile, process, and analyse statistical information regarding public health and health care in accordance with Paragraph 3 Clause 6 **of the By-laws of the Centre for Disease Prevention and Control**.[24] In that regard, the Centre carries out several tasks outlined in the mentioned bylaws. Law On the Rights of Patients, Section 10, Paragraph 7 Clause 2 requires that consent is for a particular research project and given in writing. One could question, whether it is possible to draw a clear line between public interest in the field of public health and research purposes due to how Section 10 Paragraphs 7-9 of the Law On the Rights of Patients are constructed.

14-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Latvia the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Latvia:	
Mechanism	• Application to a centralised data governance and access body (hence other than each data controller / data custodian individually) Please note that the body functions only to some degree and in some cases. • Other: Access to patient data for research purposes takes place through Section 10 of the Law On the Rights of Patients.
With regards to the "centralised data governance and access body", note that it functions only to some degree and in some cases. There are no by-laws or other regulations that have instituted exemptions to the principle that the research must first be submitted to central body. See the Procedures for Using the Patient Data in a Specific Research. See also Section 10, Paragraphs 7-9 of the Law On the Rights of Patients. With regards to Section 10 of the Law on the Rights of Patients, only if preconditions that are set forth in Section 10, Paragraph 7 of the Law to use patient data in research are not met, the application to use data shall go through the competent state authority (the Centre for Disease Prevention and Control). How access to these data is organized by individual care providers is not expressly regulated. The law does not require ethical approvals. Nonetheless, they could take place, in particular regarding publication purposes. See also the Procedures for Using the Patient Data in a Specific Research.[25] Please note that for genetic data there is a separate legal framework and is not accounted here.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Latvia did not adopt such a system.	
Legislation has been adopted 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	

[22] See the Statistics Law here. Please note that the English translation is not up to date, use the Latvian text instead.

[23] Cabinet Regulation No. 720 of 27 November 2018, Rules on model official statistical forms in the field of health care (unofficial translation) [Noteikumi par oficiālās statistikas veidlapu paraugiem veselības aprūpes jomā], Latvijas Vēstnesis, 241, 07.12.2018.

[24] See the By-law here. Please note that the English translation is not up to date, use the Latvian text instead.

[25] See the Procedures here.

Latvia has no specific legislation on this topic.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
Latvia did not adopt such a system. In principle, the system is enabled to do that (see Paragraph 4 Clause 2 of the Regulations Regarding the Unified Electronic Information System of the Health Sector. However, a procedure lacks, likewise there is only limited amount of data entered into the system.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Latvia has no specific legislation on this topic.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
The national approach to data sharing has not been thought through. Even though data access per se is possible, a procedure for accessing EHR for research purposes has not been adopted.

14-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Latvia.

Rights of the patient	How the right can be exercised in Latvia
Article 15 'right to access data concerning him or her'	• Through a formal national 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 (see below)
Direct reference to GDPR is possible, when the matter is not regulated by national law. Therefore "system" is to be interpreted narrowly *and here is interpreted as a norm that enables access*. Likewise, when so expressly provided by national law, the data subject may rely specifically on that law. See Section 11, Paragraph 1, Clause 1 of the Human Genome Research Law which sets forth a right to become acquainted or refuse to become acquainted with the data stored in the genome database regarding the gene donor. Furthermore, Section 9, Paragraph 2 of the Law On the Rights of Patients addresses the right to receive information regarding the use of the information included in his or her medical documents as set forth in law.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a formal national data rectification request system established by legislation • A patient can also request rectification from the data controller by direct reference to Article 16 GDPR
Please note that "system" is to be interpreted narrowly *and here is interpreted as a norm that enables access*. Section 9, Paragraph 3 of Law On the Rights of Patients enables rectification regarding medical data. Direct reference to GDPR is possible, when the matter is not regulated by national law.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
Procedures for Keeping Medical Documents prescribe considerable requirements concerning keeping of the medical records. In that way, the right to ask the data to be erased is considerably constrained (is close to non-existent). However, should there be any information that exceeds what shall be kept, the right to have the data erased will apply.	

Article 20 'right to data portability'	• Patients do not have a right to obtain a portable copy of medical records
• Article 20 GDPR does not apply because health data are not collected on the basis of consent and no sectoral legislation allows this • Article 20 GDPR does not apply because data processing is not carried out by automated means (e.g. no Electronic Health record)	

14-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Latvia to include data from apps and devices in the EHR. In addition, the table displays how Latvia have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. Although there is one public system, it is not fully functioning. There are also private initiatives that store patient data (e.g. analysis results), however, their use is not compulsory. An example of such a system is DATAMED. There are several systems, administered by separate ICT vendors or service providers. These private systems are not specifically regulated, but the national system is. It (the Unified Electronic Information System of the Health Sector) is set up in accordance with the Regulations Regarding the Unified Electronic Information System of the Health Sector. In the Regulation, it is specified what kind of information shall be included in this system; it also determines centralised processing of the data related to a person's health (specified in this Regulation) that is needed for medical treatment (including, electronic prescriptions in circulation between a medical practitioner and pharmacist; referrals for receipt of a health care service).	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Latvia does not yet participate in eHDSI but plans to do so by 2025.	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• No, there are no national or regional data security policies to ensure use of standards for data security.
Regulations Regarding the Unified Electronic Information System of the Health Sector set forth some standardized procedures for data exchange, however, technical requirements are not set forth in law or a public policy document. Nonetheless, as derives from the system's description, it is based on HL7 standard.[26]	
Data quality policies regarding the technical standards to be used to ensure the quality of health	

[26] See https://viss.gov.lv/lv/Eves

data for use in EHRs or other digital applications	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.
There are no technical standards as law or public policy. Only requirements regarding content of the records are regulated. See the Regulations Regarding the Unified Electronic Information System of the Health Sector.[27] These requirements are incomplete vis-a-vis data quality principles.	
Agencies which oversee the implementation of technical standards	
As there are no regional or national technical standards there is no agency to oversee it. However, it could be noted that the data controller is the National Health Service in accordance with Paragraph 2 of the Regulations Regarding the Unified Electronic Information System of the Health Sector. The question of medical documentation falls in the competences of the Health Inspectorate (Veselības inspekcija), whereas data protection matters fall in the competences of Data State Inspectorate (Datu valsts inspekcija). Technology governance is the responsibility of the Ministry of Environmental Protection and Regional Development of the Republic of Latvia [Vides aizsardzības un reģionālās attīstības ministrija]. See By-laws of the Ministry of Environmental Protection and Regional Development (unofficial translation) [Vides aizsardzības un reģionālās attīstības ministrijas nolikums] Latvijas Vēstnesis, 52, 01.04.2011, paragraph 4.1.8.	

[27] Procedures for Keeping Medical Documents sets forth rules regarding medical documents. In accordance with Paragraph 5, medical entries shall be electronically accumulated in a unified electronic information system of the health sector in accordance with the laws and regulations regarding the unified electronic information system of the health sector. Therefore, this question is regulated solely by the regulation applicable to the electronic system.

15 COUNTRY FICHE LITHUANIA

The following sections provide an overview of the rules for processing of health data currently in place in Lithuania both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[28]

15-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	There is no specific legislation. Consent for treatment is considered to be a sufficient basis for health data processing. Laws that may apply are: • Civil code of the Republic of Lithuania • Law on Health Care Institutions • Law on Health Systems • Law on the Patient's Rights and Compensation of Damage to their Health Law on Legal Protection of Personal Data. • Minister of Health issued recommended Rules for The Processing of Personal Data by the Healthcare Providers (30/11/2017, No. V-1371) . So health or care providers individually indicate bases for processing health data, following GDPR.
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Order of Minister of Health (01/02/2001, No. 65) Procedure for Providing Patient Information to Public Authorities and other Bodies.
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent • 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Adopted in 2014. The Order (Minister of Health) of the procedures for the provision of telemedicine services sets technical and managerial requirements for telemedicine services in the country. The Order applies to all healthcare providers.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• Processing app derived data for primary use is not regulated.
Specific legislation on **genetic testing**	
National legislation	Lithuania has specific regulations for genetic testing. Order of Minister of Health (02/08/2012, No. V-745) Requirements for The Provision of Genetic Personal Healthcare Services. It indicates requirement for specialist, medical devices and other equipment, facilities, when providing genetic personal health care.

[28] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Lithuania. The authors of the report take full responsibility for any interpretations in the country fiche.

15-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	The following laws apply in Lithuania: • Law on the Patients' Rights and Compensation of Damage to Health • Law on Health Systems • Law on Health Care Institutions Laws outline the purposes for which health data can be used without patient's consent. The Laws stipulate that, without the patient's consent, confidential information may be provided to state institutions (when required by the law) in accordance with the procedure established by legal acts. In all cases, the provision of confidential information must comply with the principles of common sense, integrity and protection of the rights of patients and priority of patient's interests.
Legal basis GDPR	• 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
Specific legislation addressing 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.	
National legislation	Lithuania has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Lithuania has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	The legislation that applies is the Order of Minister of Health (No. 673, 12/12/2002, last amended 25/02/2020). The Order provides a description of the procedure for registration and provision of information on the subject of compulsory epidemiological registration. The Order regulates registration of communicable diseases (deaths), communicable pathogens and their transmission, cases of bites or scratched by animals, suspected of having rabies, complications after vaccination (adverse reactions to vaccines) in health care institutions, and the procedure for providing information.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
No, it is not possible.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	

Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	The Law on the Management of State Information Resources of the Republic of Lithuania forms the basis of which state information systems are developed. Examples of created information systems and registries, in accordance with this law, are: State information systems for communicable diseases (Order of Minister of Health) State Register of Occupational Diseases (Government Resolution)
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • A healthcare professional may be given access to the data that he or she has submitted to the registry • A patient may be given access to any data concerning themselves

* Note. 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.

15-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Lithuania has no specific legislation on this topic.
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.	Lithuania has no specific legislation on this topic.

15-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Lithuania the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Lithuania:	
Mechanism	• Application to a local research ethics committee • Application to a national research ethics committee

	• The data controller provides direct access upon proof of agreement of a research ethics committee or DPA
Biomedical research in Lithuania may be performed only with an approval obtained from the Lithuanian Bioethics Committee or the Regional Biomedical Research Ethics Committee. Conduct of biomedical research without a prior approval shall be unlawful.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Lithuania did not adopt such a system.	
Legislation has been adopted 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	
Lithuania has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Lithuania did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Lithuania has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
There are no systems in place at the moment for secondary use of health data. There are some initiatives at the national level to develop such infrastructure (similar to Finish FinData solution).	

15-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Lithuania.

Rights of the patient	How the right can be exercised in Lithuania
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Lithuania has not adopted specific legislation on the application of such a right in the area of health.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Lithuania has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions
This right is linked to the right to rectification of data, correction of inaccuracies, or to cases where data were obtained without legal bases.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

15-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Lithuania to include data from apps and devices in the EHR. In addition, the table displays how Lithuania have adopted policies, guidelines or legal requirements that ensure technical

standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. Patients can access their data using ESPBI IS patient portal (www.esveikata.lt).	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs. At this point this is not possible (technical issues). However, the state is developing an app for the citizens to access their EHR on mobile devices. It might be the first step towards integrating mobile applications more into traditional EHRs.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Currently, technical work is being done in order to exchange prescriptions with other European countries. It is planned that by the beginning of 2022 we will be able to both prescribe and dispense drugs for cross border use. The Ministry of Health has also submitted an application for funds in order to exchange Patient Summary on European level.	
Technical standards	
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	
Policy level	• 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)
The Minister of Health has approved a list of requirements and specifications for integrating healthcare institutions' information systems to a central e-health system. These requirements and specifications apply to all state players. Lithuania is using the HL7 FHIR standard.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
The Minister of Health has approved list of requirements and standards for ensuring the security of central e- health system. Requirements include technical aspects, regulations for workflow and personnel. A Code of Conduct for Health Data security is currently in development. It is expected that all stakeholders and healthcare providers will endorse it and implement it.	
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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.
Agencies which oversee the implementation of technical standards	
The Ministry of Health of the Republic of Lithuania oversees implementation of technical standards.	

15-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Hospital and medical specialist care	http://www.hi.lt/traumu-ir-nelaimingu-atsitikimu-stebesenos-is-poskyris.html : Injury and accident monitoring information system

16 COUNTRY FICHE LUXEMBOURG

The following sections provide an overview of the rules for processing of health data currently in place in Luxembourg both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[29]
In Luxembourg legislation concerning the health sector can be found in the *Code Santé* via http://legilux.public.lu/eli/etat/leg/code/sante/20200608. For the purposes of this Luxembourg related part of the survey, unless indicated otherwise, all references to acts that can be found in the *Code Santé*.

16-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The **Act on the Rights and Obligations of Patients** [*Loi du 24 juillet 2014 relative aux droits et obligations du patient, portant création d'un service national d'information et de médiation dans le domaine de la santé*] is *inter alia* applicable to health care providers (prestataires de soins). • Section 3, Article 15(1) provides that health care providers establish a patient file. This provision further establishes the legal basis for a grand-ducal regulation that specifies the minimum content of such patient files. To date no such regulation has been adopted. Further, Article 15(2) requires that health professionals see to it that their individual instructions, prescriptions and services are being documented in the patient file. Patient files need to be kept for a period of at least ten years, starting from the end of the respective treatment. Neither the patient nor the health professional has the right to erase information from the file, rectifications are possible under certain conditions (Article 15(5)). • Article 16 regulate the patient's right to access his/her file and: to be provided explications (para. 1); to receive copies (para. 3); determines a deadline within which the health professional has to provide access (15 working days) (para. 4); and specific rules are being established for cases in which the access to the patient file might constitute a risk to the patient (para. 5). • Article 17 provides that the health professional's personal comments, which include inter alia his/her impressions and reflections may not be shared with the patient. Personal data of third persons are never shared with the patient. • Article 18(1) provides for an exception to the medical secrecy, protected by criminal law, in that it allows health professionals to share information with relatives of the patient, provided the latter consents to that measure. Such consent is not necessary in cases where the patient is no longer able to mark his/her consent and had not opposed him-/herself beforehand. • Article 19(1) establishes the right of close family members to access the patient's file and to data related to his/her health. According to para. 2, parents of a minor and every other person with parental authority dispose of the same right of access. In both cases, the person concerned is vested with the right to refuse. The **Act on Hospitals and Hospital Planning** [*Loi du 8 mars 2018 relative aux*

[29] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Luxembourg. The authors of the report take full responsibility for any interpretations in the country fiche.

	établissements hospitaliers et à la planification hospitalière] • art. 37 provides for the duty on the side of hospitals to keep patient files. These need to be in line with the minimum requirements set up by grand-ducal regulation[30] . According to the same article, the rules enshrined in the Act on the Rights and Obligations of Patients (see supra) also apply to patients of hospitals. • The act's art. 38 para. 4 foresees that every hospital needs to create an administrative structure dedicated to the processing of medical data (service de documentation médicale) whose tasks consist notably in the collection, the processing and the treatment of medical data and their safeguarding during a period of ten years. The **Act on Euthanasia and Assisted Suicide** [*Loi du 16 mars 2009 sur l'euthanasie et l'assistance au suicide*] • Art. 8 provides in its art. 7 that the medical doctor performing an act of euthanasia needs to submit a form to the Commission on the Control and Evaluation of that law ("the Commission"), providing certain pieces of patient data. The data needs to be presented in the form of two distinct documents, both being of confidential nature. The first document needs to be submitted by way of sealed envelope and contains the personal information of the patient (name and residence), of the medical doctor who submits the document and potential other medical doctors that have been consulted by the patient, etc. The second document contains information on the disease the patient suffers from, the nature of his/her suffering, the elements that allow for the conclusion that the suffering is unbearable and without reasonable chance of improvement, etc. • The Commission first examines the latter document and in case of doubt can decide to also access the former, thereby putting aside anonymity. The Commission's role in the context of this act is to ascertain whether the preconditions for the performance of an act of euthanasia are met. A positive decision is precondition for the performance of such act. In the wider scope of things, it might also be of interest that the Medical-legal documentation service (Unité de documentation medico-légale) which forms part of the National Health Laboratory (Laboratoire national de santé) is charged with providing any person that has fallen victim of a criminal act that resulted in physical harm, the corresponding medical-legal documentation. This document can in principle be archived for a maximum period of ten years, starting as of its drafting (a prolongation being admissible in anonymised form and for predefined purposes, such as reaserach, only); see art. 2-1 of the Act on the Creation of the National Health Laboratory (Loi du 7 août 2012 portant création de l'établissement public «Laboratoire national de santé»).
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	The most important legislation is: • The **Act on the Rights and Obligations of Patients** Article 18(2) constitutes the right of two or more healthcare professionals to exchange information relating to a patient in order to assure continuity of care or to determine the best possible treatment. The same provision constitutes that, in cases of hospital treatment, the patient's data is to be considered entrusted by the patient to the entire medical team responsible for the treatment. The person concerned is vested with the right to refuse. • The **Grand Ducal Regulation on the Shared Care Record** [*Règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé]*, notably its Article 6 in conjuction with the annex to the grand ducal regulation, defines that the treating medical doctor has the right to access

[30] Grand ducal regulation determining the minimum content of patient files of hospital patients, available here: http://legilux.public.lu/eli/etat/leg/rgd/2019/01/13/a48/jo (last visited on the 1st of July 2020).

	the documents and files that are saved in the system of electronic patient files that has been set up by this very legislative act (and which does not replace the "classical" patient file).
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Luxembourg has no specific legislation on this topic. For the sake of completeness mention should be made of the fact that, even though no such legislation exists, in the wake of the SARS-CoV-2 pandemic specific legislation has been adopted in order to allow for measures that are deemed to restrict propagation of the virus to a minimum. These legislative acts include: • The **Grand-ducal Regulation of the 17th of March 2020** [*Règlement grand-ducal du 17 mars 2020 modifiant le règlement grand-ducal modifié du 21 décembre 1998 arrêtant la nomenclature des actes et services des médecins pris en charge par l'assurance maladie*] which lays the basis for medical consultations performed via electronic means by assuring their reimbursement by the public social security bodies. • The **Grand-ducal Regulation of the 28th of April 2020** [*Règlement grand-ducal du 28 avril 2020 portant modification du règlement grand-ducal modifié du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19*] which lays down that throughout the pandemic teleconsultation should be given priority over face-to-face consultation by medical doctors. However, none of these legislative instruments includes specific provisions on the processing of health data.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• Other combination: 6(1)(a) Consent + 6(1)(c) legal obligation.
Specific legislation on **genetic testing**	
National legislation	Luxembourg has specific regulations for genetic testing. Article 6(3) of the **Act on Hospitals and Hospital Planning** provides that a ministerial authorisation for the performance of testing of human genetics can exclusively be issued vis-à-vis the National Health Laboratory. It also defines the activity referred to by this provision. This is corroborated by Article 1(3) of the **Act on Medical Laboratories** [*Loi modifiee du 16 juillet 1984 relative aux laboratoires d'analyses medicales*], which contains a provision to the same effect by prohibiting any such testing be performed by other medical laboratories. The **Act on the Creation of the National Commission for Data Protection** Article 66 forbids the treatment of genetic data for the purposes of the exercise of rights of the controller with regard to the fields of labour law and insurance law.

16-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health

authorities	
National legislation	The main set of legislative rules can be found in the **Act on Hospitals and Hospital Planning**. Article 3 sets out that the respective Minister of Health evaluates the needs in terms of health care and bases this evaluation on the so called *carte sanitaire*. This documents comprises, *inter alia*, data on the reason why patients received stationary or ambulant treatment at a hospital (see para. 2). In the framework of this evaluation the Minister also takes other aspects into consideration (see para. 1). Further, the same act's art. 38 establishes the obligation of every hospital to perform a quantitative and qualitative analysis of its activity. This rests on data that is collected during every stationary or ambulant treatment and include the reason for the hospital treatment, the type of medical treatment and examinations performed, the prescriptions issued, etc. (see para. 2).
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation addressing 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.	
National legislation	Luxembourg has no specific legislation on this topic. However, Art. 37. (3) of the **Act on Hospitals and Hospital Planning** open a door on further processing.
Specific legislation addressing 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**	
National legislation	Luxembourg has legislation on this topic, but indirectly. Art. 45.-5 Collaboration du corps médical et des patients, *Règlement grand-ducal du 10 septembre 2012 modifiant le règlement grand-ducal modifié du 15 décembre 1992 relatif à la mise sur le marché des médicaments et le règlement grand-ducal modifié du 19 novembre 2004 concernant la fabrication de médicaments, les bonnes pratiques de fabrication de médicaments et les bonnes pratiques de fabrication de médicaments expérimentaux à usage humain.*
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	The **Act on the Obligatory Declaration of Certain Illnesses in the Framework of the Protection of Public Health** [*Loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique*] which notably aims at identifying illnesses that require urgent and international action. The Act establishes the obligation of medical doctors, dentists and medical laboratories to inform the health authorities about cases of those illnesses defined in a separate grand ducal regulation. This legal act[31] contains a number of annexes that set out the different illnesses that fall within its scope of application.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, this is possible at national level as the institution dealing with communicable diseases is the health authority – see **Act on the Obligatory Declaration of Certain Illnesses in the Framework of the Protection of Public Health.** At EU and international level, it is not possible.	
Legal basis used for national level specific legislation that has been enacted about other cross-	

[31] Grand ducal regulation enumerating the illnesses to which obligatory declaratzion applies, available here: http://legilux.public.lu/eli/etat/leg/rgd/2019/02/15/a104/jo (last visited on the 6th of July 2020).

border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Luxembourg has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	See the *Règlement grand-ducal du 18 avril 2013 déterminant les modalités et conditions de fonctionnement du registre national du cancer.*
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • Anonymised data can be accessed by third parties (see article 8 of the above mentioned legislation), but there are no actors specifically mentioned.

* Note. 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.

16-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Luxembourg has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes
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.	Luxembourg has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes
National legislation	In Luxembourg, the legislation does not differentiate between not for profit researchers and for profit researchers. The Act of 1 August 2018 on the Organisation of the National Data Protection Commission and the general data protection framework, Chapter 2 regulates data Processing for the purposes of scientific or historical research or statistical purposes.

16-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Luxembourg the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Luxembourg:	
Mechanism	• Application to a national research ethics committee • The data controller provides direct access upon proof of agreement of a research ethics committee or DPA
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Luxembourg did not adopt such a system.	
Legislation has been adopted 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	
Luxembourg has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Luxembourg did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Luxembourg has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
To our knowledge, there is no formal official infrastructure in place.	

16-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Luxembourg.

Rights of the patient	How the right can be exercised in Luxembourg
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Article 16 of the Act on the Rights and Obligations of Patients states that patients can request access to their record and health data. As the law is dated from 2014, it is not in application of Article 15 GDPR, but it is linked.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Luxembourg has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions
Luxembourg has not adopted specific legislation on the application of such a right in the area of health.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

16-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Luxembourg to include data from apps and devices in the EHR. In addition, the table displays how Luxembourg have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
• This is organised nationally. The Dossier Soins Partagé (DSP) is the EHR system of Luxembourg.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Luxembourg participates in eHDSI through sharing summary records and prescriptions.	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• No, there are no national or regional data security policies to ensure use of standards for data security.
However, Article 10 of the *Règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé* lists the minimum security measures to be applied to the supporting plateform.	
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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.
Agencies which oversee the implementation of technical standards	
There is no agency that oversees this.	

17 COUNTRY FICHE HUNGARY

The following sections provide an overview of the rules for processing of health data currently in place in Hungary both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[32]

17-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The fundamental rules of data protection are set down in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ("**Privacy Act**" or "Information Act"). The fundamental piece of sector specific legislation is Act XLVII of 1997 on the Processing and Protection of Health Care Data and Related Personal Data ("**Medical Data Act**"). Art. 4(1) defines the purpose of processing medical data and related personal data: • promoting the protection, improvement, maintenance of health • promoting the efficient healthcare activity of healthcare providers, including its supervision • follow-up of the health status of the data subject • taking necessary measures in the interest of public health and epidemiology • realising patient rights Article 4(2) provides that medical data and related personal data can be processed for further if it is prescribed by other laws (acts). Those purposes are listed by para (2) in 27 points e.g. medical education and training, organisation of healthcare, statistical surveys, scientific research, exercise of official authority, social insurance, prescription of medicines and medical devices, criminal investigations, etc. Under Section 12(1), providing personal data concerning health and identifying data by the data subject is voluntary. Para (2) and (3) add that voluntariness (i.e. consent) is presumed if the data subject (patient) turns to the healthcare provider voluntarily, as well as in case of urgency or the incompetency of the data subject.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care • Other combination: Presumed consent i.e. an opt-out approach.
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	The main sector specific legislation is Medical Data Act which contains several rules on sharing health data. Under the title data processing for the purpose of healthcare, Section 7 provides that data controllers are not bound by medical secrecy if the data subject or his/her representative gives a written consent (but only within the limits of the consent) or sharing medical or personal data is a legal obligation. Further Sections provide for

[32] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Hungary. The authors of the report take full responsibility for any interpretations in the country fiche.

	specific cases of sharing data e.g. for the purposes of public health, epidemiology, occupational health, storing data in national health databases and disease registries (medical registries), and public administration.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Hungary has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	Hungary has specific regulations for genetic testing. Genetic testing is regulated by Act XXI of 2008 on the **Protection of Data on Human Genetics, on the Rules of Research and Examinations of Human Genetics and of the Functioning of Bio-banks**. Under Section 12, human genetic research can only be carried out by healthcare providers having a license of operation and which meet the minimum technical conditions, as well as the legal requirements on storing genetic samples and data. Further detailed rules are included in the following ministerial decrees: • **Decree No. 23/2002** of the Minister of Health on medical research involving human subjects. • **Decree No 60/2003** of the Minister of Health on the minimum technical requirements for the provision of healthcare services • **Decree No. 35/2005** of the Minister of Health on the clinical trial and application of correct clinical practices of investigational medicinal products intended for use in humans The applicable law and decrees set up a comprehensive legislative regime that covers the key aspects of genetic testing which can also include provisions related to personalised medicine.

17-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Section 4 of the Medical Data Act lists the purposes of processing data. Under para (2), points b), w), x), y), z), health and related personal data can be processed, in cases defined by law, for the following purposes: • epidemiological survey or analysis, • planning and organisation of healthcare, • planning costs, • organising patient pathways, • assessment and development of the quality of healthcare services, • review and development of the evaluation aspects of healthcare services,

	• measurement and evaluation of the outcomes of the healthcare system. Section 19 para (1) and (2) add to the above points that the Minister of Health and national or regional health authorities or institutes can process, within their competence, for the period and to the extent necessary to implement their tasks, the health data of the subjects (patients), as well as their social insurance number, gender, date of birth and postal code, without linking them to other personal data. Healthcare providers are obliged to share these data with the above mentioned authorities or institutes. The detailed rules are included in **Decree No. 76/2004** of the Minister of Health and Social Affairs on the range, collection and processing of certain depersonalised data in the health sector.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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.	
National legislation	Section 4 of the Medical Data Act lists the purposes of processing data. Under para (2), points s) and v), health and related personal data can be processed, in cases defined by law, for the following purposes: • continuous and safe provision of prescription medicines and medical devices • defining the efficiency and financing medicinal products and medical devices receiving outcome based funding. These provisions, in principle, include marketing authorisation, however, in practice, personal health data are not really used in the market approval procedures.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	Act XCV of 2005 on **Medicinal Products for Human Use**, Section 18 para (1) and (2) provide that the holders of market authorisation, as well as healthcare professionals are obliged to report all side effects noted to the National Institute of Pharmacy and Nutrition.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) healthcare
Specific legislation addressing 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**	
National legislation	Section 5 of the Medical Data Act, para (3) states that the persons exposed to public health or epidemiological threat are obliged to share their health and personal data, as well as their telephone number or electronic contact details with their physicians, the medical officers, epidemiological inspectors or other authorities, or WHO employees responsible for the implementation of the IHR. The IHR was promulgated by Act XCI of 2009.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. According to Section 15 of the Medical Data Act , healthcare providers shall immediately forward the health and related personal data to the health authority in case of the detection or suspect of infectious diseases listed in Annex 1 point A of the Act. In case of diseases listed in Annex 1 point B or diseases not listed in Annex, only the health data shall be reported without the related personal data but the health authority may request the personal data except for anonym HIV tests. The same rules apply in case of positive results of microbiological tests. The same data shall be reported to the authorities with epidemiological competence.	

Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	The detailed rules of disease registries (or medical registries) are included in the following pieces of legislation: • Medical Data Act, Sections 16, 16/A, 16/B, 16/C, 22/A, 22/B, 35/L • **Decree No 49/2018** of the Minister of Human Capacities on diseases with a high public health significance or high cost burden, the nomination of disease (medical) registries, and the rules of reporting and registration of such diseases
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) healthcare
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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 • 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 • Public sector researchers • Private researchers

* Note. 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.

17-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Hungary has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes
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.	Hungary has specific legislation on this topic. Legal basis: • Article 9(2)(j) research purposes

National legislation	In Hungary, the legislation does not differentiate between not for profit researchers and for profit researchers. Scientific research is listed among the purposes of data processing under Section 4 of the Medical Data Act. The special rules for research are included in Section 21 of the Medical Data Act. 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 under the general rules of the Privacy Act.

17-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Hungary the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Hungary:	
Mechanism	• Application to a local research ethics committee • Application to a national research ethics committee
In some cases a Data Protection Impact Assessment is necessary. The general rules of medical research involving human subjects are laid down by **Act CLIV on Health (Health Act)**, Sections 157-164/D. Special rules are included in Decree No. 23/2002 of the Minister of Health on biomedical research involving human subjects. In order to carry out medical research, the approval of the national and local ethics committees, as well as the given healthcare institution is always needed. The research plan is approved by the Medical Research Council. The research plan shall be approved for implementation by the executive of the healthcare institution, or in the case of another health service provider. The decree referred to above lays down special rules on the protection of persons taking part in the research, providing information about and giving consent to the research, the institutional research ethical committee and the Regional Research Ethical Committee, reporting obligation, provisions on examinations without intervention.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Hungary did not adopt such a system.	
Legislation has been adopted 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	
Hungary has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Hungary did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Hungary has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data	

for research purposes (function 2 or function 3)
The national eHealth Space and the database of the National Health Insurance Fund could in principle be a source of data for researchers. From the two, the National Health Insurance Fund's database which includes mainly healthcare financing information is available for research upon request. The national eHealth Space's dataset would be a more comprehensive data source but the legislative framework on how to use it for research purposes is not yet fully in place. Researchers can also have access to the databases of individual healthcare providers with the permission of the director or the DPO. The National Healthcare Service Centre as the operator of all public hospitals in the country has its own database. Especially university clinics (there are four medical faculties in Hungary) have significant databases.

17-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Hungary.

Rights of the patient	How the right can be exercised in Hungary
Article 15 'right to access data concerning him or her'	• Through a formal national data access request system established by legislation • A patient needs to request access from the data controller by direct reference to Article 15 GDPR
The national eHealth Space (or Electronic Health Cooperation Service Space) was established by Chapter III/A of the Medical Data Act. The detailed rules of the eHealth Space are given by **Decree No. 39/2016** of the Minister of Human Capacities. The eHealth Space contains the medical data and related personal data of all individuals in Hungary having a social insurance i.e. basically the whole population. Patients have access to their own medical records electronically. Furthermore, patients also have the option to request their medical data or records from the healthcare providers where the diagnosis or treatment was carried out, under Section 24 of Act CLIV on Health (Health Act). Healthcare providers are obliged to issue a copy of the medical record, report, medical image, etc.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a formal national 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 Health Act, Section 24, and the Medical Data Act, Section 35/J paragraph (5) apply.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
The national legislation does not contain provisions for the deletion of health data by the patient.	
Article 20 'right to data portability'	• through a formal national 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
The Health Act section 24 applies.	

17-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Hungary to include data from apps and devices in the EHR. In addition, the table displays how Hungary have adopted policies, guidelines or legal requirements that ensure technical

standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. There are two national EHR systems and several local systems. One EHR system is the database of the National Health Insurance Fund collects and cumulates all healthcare services provided to the insured persons. The aim of the database is to collect and store information for the purposes of financing medical services. The second system is the national Electronic Health Service Space (or National eHealth Infrastructure). It is based on the Medical Data Act, Chapter III/A and **Decree No. 39/2016** of the Minister of Human Capacities on the detailed rules of the eHealth Space. The eHealth Space became operational in November 2017. The modules of the eHealth Space are the following: e-prescription, e-medical history (EHR repository), event catalogue, e-referral, e-profile. The plan is that the eHealth Space will also serve as the single gateway to share data between healthcare providers but currently this is not the practice. Patients can access their health data at the national eHealth Space. Based on data protection rights, every patient have access to their health care information online via the Patient Portal. To tune privacy settings is possible by Government Customer Service administrators personally or through the Electronic Client Gateway. Healthcare data are accessible via the portal of National Health Insurance Fund, too. Patients can check the healthcare services they received in the past, as well as medicines prescribed, through their personal electronic access to the Governmental Portal and with their social insurance number. However, this database includes only the list of health services (diagnosis, treatment, prescriptions) received by the patients, not full their health records. However, the health and digital literacy of patients/citizens also needs further development.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so This is a very complex issue, including aspects like knowledge and willingness both on the patients' and the healthcare professionals' side, workload of the healthcare service, or infrastructure.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Hungary plans to participate in eHDSI with sharing prescriptions and patient summaries by 2025. Hungary has been an active member of the EU eHealth Network, as well as a partner in the EU eHealth Joint Actions including JASEHN and eHAction, and in this way participated in the creation of eHDSI.	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
The legal base of data security is Act L of 2013 on the electronic security of state and local government organizations ("**Cybersecurity Act**"). The scope of the act includes data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements.	

In order to protect electronic information systems and data, proportionally to the risks, the Act states that the electronic information systems must be allocated to particular security classes. This classification is based on confidentiality, integrity and availability properties on a scale of 1 to 5, where 5 is the highest security level.

Level 5 is applicable to data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law. The national eHealth Space falls under Level 5.

Further relevant pieces of legislation are the following:

- Government **Decree No. 187/2015** on the competence of the authorities responsible for the security inspection of electronic information systems
- Government **Decree No. 271/2018** on the tasks and powers of incident handling centres, and laying down rules for the handling and technical investigation of security incidents and the conduct of vulnerability assessments
- **Decree No 7/2013** of the Minister of National Development on the contracts of the organisations using centralised information or electronic communication services
- **Decree No. 41/2015** of the Minister of Interior on technology aspects of the Cybersecurity Act and classification rules

The standards used are ISO/IEC 27001 and ISO/IEC 27002.

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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.

Agencies which oversee the implementation of technical standards

The National Cyber Security Centre is the competent authority covering the lifecycle of the electronic information systems, including the planning phase, regulation, control and incident handling. The National Cyber Security Centre includes the National Electronic Information Security Authority, GovCERT-Hungary for incident handling issues, and the Unit responsible for the security management and vulnerability assessment.

As regards data protection competence, the National Authority for Data Protection and Freedom of Information is responsible for monitoring and promoting the enforcement of the right to the protection of personal data and the right to freedom of information including access to data of public interest and data accessible on public interest grounds, as well as promoting the free movement of personal data within the EU.

17-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	Public Health Focused Model Programme for Organising Primary Care Services Backed by a Virtual Care Service Centre - Swiss-Hungarian Cooperation Programme https://semmelweis.hu/emk/en/projects/closed-projects/sh- 8-1-swiss-hungarian-cooperation-programme/
Hospital and medical specialist care	Innohealth Datalake Project https://innohealth.eu/en/datalake/ Inclouded Development Centre https://u-szeged.hu/download.php?docID=51795
Self measurements	http://menta.gov.hu/en

18 COUNTRY FICHE MALTA

The following sections provide an overview of the rules for processing of health data currently in place in Malta both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[33]

18-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	1) **The Charter of Patient's Rights and Responsibilities**, as issued by the Malta Ministry for Health, sets out *inter alia* the essential privacy and confidentiality rights to which patients are entitled to expect from their healthcare providers. 2) Healthcare professionals are also generally subject to duties of professional secrecy in terms of the **Professional Secrecy Act**, Chapter 377 of the laws of Malta combined with article 257 of the **Criminal Code**, Chapter 9 of the laws of Malta. 3) The Processing of Personal Data (Secondary Processing) (Health Sector) Regulations Subsidiary Legislation 528.10 (**Public Health Act, SL 528.10**), also provides for the conditions on which secondary processing of health data may take place, together with access to health data for such purposes. Processing health records for any purpose other than those set out in the SL 528.10 requires the consent of the data subject concerned as provided for in the GDPR.
Legal basis GDPR	• 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)(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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	SL 528.10 permits the processing of personal data (and therefore sharing) for secondary purposes where such processing is related to: 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; b. 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; c. The monitoring of contractual obligations, including the purposes of quality control, management information and monitoring of such services

[33] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Malta. The authors of the report take full responsibility for any interpretations in the country fiche.

	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; d. 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; e. 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; f. The investigation and monitoring of health threats, which typically requires the processing of health record data for the protection of public health; and g. Access to health records, for the purpose of research activities.
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Malta has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	Malta does not have specific regulations for genetic testing.

18-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	SL 528.10 – elaborated on in the previous paragraph.
Legal basis GDPR	• 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 • Other combination: on the basis of the conditions set out on in SL 528.10, which *inter alia* require prior consultation and authorization from the local data protection authority (DPA)
Specific legislation addressing 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.	
National legislation	Clinical testing information must however be provided in order to obtain a marketing authorisation pursuant to the **Subsidiary Legislation 458.34 Medicines (Marketing Authorisations) Regulations** (SL 458.34). The Schedule to SL 458.34 stipulates the various criteria and standards which are to be abided by in respect of testing of medicinal products and data submitted in connection with marketing authorisation applications.
Legal basis	• Other combination: 6(1)(a) consent and 9(2)(a) consent

GDPR	
Specific legislation addressing 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**	
National legislation	**Subsidiary Legislation 458.35 Pharmacovigilance Regulations** (SL 458.35) regulates the use of authorised medicinal products for humans and pharmacovigilance activity connected therewith.
Legal basis GDPR	• 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
Specific legislation addressing 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**	
National legislation	Malta has no specific legislation on this topic.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
There is no specific legislation on this point, therefore this issue is mostly dealth with on an ad hoc basis. The Infectious Disease Prevention and Control Unit (IDPCU) is tasked with surveillance of infectious diseases. The overarching legislation is the Public Health Act. SL 528.10 permits the processing of personal data (and therefore sharing) for secondary purposes, including for the investigation and monitoring of health threats, which typically requires the processing of health record data for the protection of public health.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	Malta has not adopted specific legislation on this topic, but the legal basis that is mostly relevant and applied is: • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
Legal basis GDPR	• 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
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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 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 • Public sector researchers • Private researchers Generally healthcare professionals would have access, however, the information pertaining to other patients who are not under their care would be anonymised.

* Note. 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.

18-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Malta has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
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.	Malta has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
National legislation	In Malta, the legislation does not differentiate between not for profit researchers and for profit researchers. SL 528.10 permits the processing of personal data (and therefore sharing) for secondary purposes, including for scientific or historical research. Access to health records for research purposes as listed in SL 528.10 can only take place if the personal data has been anonymised. If, however, such processing cannot be conducted using anonymised data, then the authorisation of the IDPC and the Health Ethics Committee within the Ministry of Health is required. Where granted, the processing of such data must be conducted using pseudonymised data, and where this is not possible appropriate measures are taken to safeguard the rights and fundamental freedoms of the data subject by providing that data should be anonymised as soon as the research or the statistical study no longer require identifiable data.

18-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Malta the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Malta:	
Mechanism	• Application to a centralised data governance and access body (hence other than each data controller / data custodian individually)
There are no exemptions to the principle that the research must first be submitted to the application body.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Malta did not adopt such a system.	

Legislation has been adopted 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
Malta has no specific legislation on this topic.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
Malta has adopted a system to facilitate this. SL 528.10 allows for the re-use of health record data for secondary purposes.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Privately funded researchers are not obliged but may choose to do so.
Data access infrastructure 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 The EHR are managed by the Directorate for Health Information and Research[34] which is run through the Ministry of Health. Through this, a person can request information. Depending on whether the data request pertains to aggregate data or record level data, different forms will need to be submitted. Applications are vetted by the DHIR prior to release of the relevant information.

18-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Malta.

Rights of the patient	How the right can be exercised in Malta
Article 15 'right to access data concerning him or her'	• Through a formal national data access request system established by legislation • A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Patients can access their data via the national data system MyHealth Portal.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a formal national data rectification request system established by legislation • A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Patients can rectify their data via MyHealth Portal.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• The law is not clear on this issue.
The legislature has adopted **Subsidiary Legislation 586.09 Restriction of the Data Protection** (obligations and rights) Regulations (SL 586.09) which provides for a restriction to Article 23 GDPR where such restrictions are a necessary measure required in respect of, *inter alia*: (a) for the safeguarding and maintaining of national security, public security, defence and the international relations of Malta; (b) health data that is processed and where it would be likely that the application of the rights and obligations referred to in article 5(1) of the Act would cause serious harm to the vital interests	

[34] https://deputyprimeminister.gov.mt/en/dhir/Pages/About-us.aspx

of the patient. It can be argued that the exemption under 'b' can be interpreted very broadly.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

18-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Malta to include data from apps and devices in the EHR. In addition, the table displays how Malta have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. The 'myHealth' Portal allows Maltese citizens to view their medical records and also give permission to their doctors to view the same. Information can be accessed on case summaries, upcoming appointments, POYC (pharmacy of your choice) entitlement and, when released, laboratory results and medical imaging reports. Interaction with a patient's doctor is also possible.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Malta participates in eHDSI through sharing summary records.	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• No, there are no national or regional data security policies to ensure use of standards for data security.
There are no *written* national or regional data security policies. The Ministry of Health specifies that the data held within the Government information management system ensures the highest possible level of security for data, however, it is unclear which standards are employed.	
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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.
Agencies which oversee the implementation of technical standards	
There is no agency that oversees the implementation of technical standards.	

18-7 National examples of organisations and registries on secondary use of health data

National example
Directorate for Health Information and Research (DHIR) https://deputyprimeminister.gov.mt/en/dhir/Pages/Introduction.aspx The DHIR is largely responsible for secondary processing of personal data and is required to access personal data from public and private health care entities as well as notifications by healthcare providers.

19 COUNTRY FICHE THE NETHERLANDS

The following sections provide an overview of the rules for processing of health data currently in place in the Netherlands both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[35]

19-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The Dutch **Act on Medical Treatment Contracts** (WGBO) regulates the relationship between patients and care providers. In addition, Article 30.3 of the Dutch **Executing Act of the GDPR** (UAVG) applies.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	According to the WGBO, patient data may be shared amongst the treatment team of the patient at the health care provider. Consent is needed to send data to another health care provider. If the patient is referred and has agreed with the referral, consent is presumed. In the case of electronic exchange of patient data between healthcare providers, where the data maybe accessed by a new health care provider, the **Additional Provisions on the Processing of Personal Data in Healthcare Act** (WABVPZ) requires in article 15.a that the patient should explicitly consent to making data available via so-called pull systems.
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	The Netherlands has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	The Netherlands has specific regulations for genetic testing. Specific regulations for genetic testing are specified in the **Specialist Medical Procedures Act** (WBMV). Only 6 laboratories are officially allowed to perform genetic testing. However, other laboratories at hospitals can act as the satellite centres.

[35] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in the Netherlands. The authors of the report take full responsibility for any interpretations in the country fiche.

19-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	The **Health Insurance Act** (ZVW) requires health care providers to submit certain claims codes of the treatment given to a patient to health insurers in order to get paid. The **Healthcare Market Regulation Act** requires health care providers to submit pseudonymised data to the Dutch Health Care Authority (NZa). The NZa further processes the data and sends statistics to the Department of Health. Health care providers are also obliged to submit data about treatments etc. to Statistics Netherlands. However, this is not always effectuated if Statistics Netherlands receives the data via other sources such as via the Health Care Authority.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation addressing 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.	
National legislation	The Netherlands has no specific legislation on this topic, when personal data are regarded.
Specific legislation addressing 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**	
National legislation	The Netherlands has no specific legislation on this topic, when personal data are regarded.
Legal basis GDPR	• There is no specific legislation, hence the legal basis can only be consent
Specific legislation addressing 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**	
National legislation	The Public Health Act (WPG).
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible to the National Institute for Health and the Environment, not to the ECDC. Article 28 of the Public Health Act regulates this.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(i) public interest in the field of public health. The original data collection by the health care provider will be based on consent.
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	

National legislation	The Netherlands has no specific legislation on this topic.
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • In the absence of legislation the usual rules based on the GDPR apply and the Dutch legislation concerning research (see the next section). The submitting doctors usually always have access to the data they submitted. The data may be used for research if an access committee or privacy committee instituted by the registry holder has agreed to the data being used. As the registry is usually based on the public interest exception for research, the research should be in the public interest.

* Note. 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.

19-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	The Netherlands has specific legislation on this topic. Legal basis: • 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.
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.	The Netherlands has specific legislation on this topic. Legal basis: • 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.
National legislation	The legislation regulating access by third-party public-sector researchers consists of the Act on the Treatment Contract (with article 7:458 Civil Code providing an exception to medical confidentiality in the case of research), the GDPR and the Act executing the GDPR (with article 24 providing an exception for the new controller to the consent principle in the case of research with data). When data is used for research by third-party public-sector researchers, Article 24 of the UAVG applies, and the legal base should be consent or an exemption which must fulfil the following conditions: • It is impossible or not feasible to ask for consent • The data are pseudonymised • The research serves a public interest • The patient did not in general opt-out for such use (article 7:458 of the treatment contract) The mentioned Acts do not distinguish between public or not public researchers. However, when using the exemption to the consent principle the research must amongst other things be in the public interest. The criterion will be more difficult to meet by researchers from commercial enterprises.

19-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In the Netherlands the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in the Netherlands:	
Mechanism	• The data controller provides direct access without engagement to an ethics committee or DPA
As there is no centralised data governance and access body, the data governance models differ between controllers, repositories.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
The Netherlands did not adopt such a system.	
Legislation has been adopted 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	
The Netherlands has no specific legislation on this topic. However, in practice the public funders of research require that data are processed in a way that ensures the FAIR principles, which is required through explicit conditions in their funding agreements.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
the Netherlands did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Privately funded researchers are not obliged but may choose to do so.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
• There are several national systems to share data for secondary use. • There are several sector specific national systems to share data for secondary use. • 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. The Netherlands has a fragmented data access infrastructure. There are many data repositories, registries, some national some regional, some for specific diseases, some for specific health care sectors, some run by research institutes, universities, some run by ICT vendors.	

19-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in the Netherlands.

Rights of the patient	**How the right can be exercised in the Netherlands**
Article 15 'right to access data concerning him or her'	• Other: The right to access has been laid down in sectoral health legislation.
Relevant legislation on such a right in the Netherlands is provided in • the Act on Medical Treatment Contracts (WGBO)	

• the Additional Provisions on the Processing of Personal Data in Healthcare Act (WABVPZ)	
Article 16 'right to rectify any inaccurate data concerning him or her'	• The right to rectification is restricted based on sectoral legislation adopted in accordance with Article 23(1)
Relevant legislation on such a right in the Netherlands is provided in • The WGBO, preceding the GDPR, explicitly did not confer the patient a right to rectification in order to avoid discussions about the content of the medical file which should be based on professional considerations. The patient has the explicit right to add his/her own notes to the medical files	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions
Relevant legislation on such a right in the Netherlands is provided in • The WGBO, the request can be denied if retention of the file is in the interest of another party than the patient.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

19-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in the Netherlands to include data from apps and devices in the EHR. In addition, the table displays how the Netherlands have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. As of 1 July 2020 all citizens must have direct online access to their GP EHR by law. A set of technical rules and regulations has been established (medMij) for patients to export the data from the EHR into a personal health space.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• Healthcare professionals are allowed to incorporate patient generated data into healthcare professional/ provider held EHRs. There is no standard system in the Netherlands as to how incorporate these data.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
The Netherlands does not yet participate in eHDSI but plans to do so by 2025.	
Technical standards	
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	
Policy level	• 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) • 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)
The Dutch ministry's information council (informatieberaad) stimulates interoperability and there are many initiatives to enhance interoperability in all health care sectors.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care).
A Royal Decree originally based on the implementing act of Directive 95/46/EC and now based on article 15(j) of the Act on Additional Conditions to Process Personal Data in Health refers to the norms on data security in health set by the Royal Dutch Standardisation Institute. NEN-7510 is the security standard for the health sector.	
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	
Policy level	• There are several national data quality policies which address use of standards for each healthcare provider sector (primary, secondary, tertiary, long term care)
Data quality is generally seen as a key issue in the reuse of data, and there are and have been national policies for specific sectors. For example, GPs pay for performance fees based on their quality of recording in their EHR systems, which have been evalutated by Nivel. There have been other initiatives in other healthcare fields. Standardization of EHRs has been on the agenda of Nictiz, the national health & ICT institute.	
Agencies which oversee the implementation of technical standards	
There is no separate agency which oversees the implementation and can take measures in case of non-implementation. However, the Department of Health has announced to take more control over the development of standards. If those would be laid down in legislation, the Inspectorate for Health and Youth will control their implementation.	

19-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	Nivel Primary Care Database https://www.nivel.nl/en/nivel-primary-care-database
Hospital and medical specialist care	Dutch Hospital Data (DHD) www.dhd.nl
Prescription drugs	Dutch Institute for Rational Use of Medicine (IVM); Nivel Primary Care Database https://www.medicijngebruik.nl/english; https://www.nivel.nl/en/nivel-primary-care-database

20 COUNTRY FICHE AUSTRIA

The following sections provide an overview of the rules for processing of health data currently in place in Austria both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[36]

20-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	With regards to personal data protection in healthcare, besides GDPR and the Federal Act on the protection of personal data (DSG), at least 25 acts are relevant. Some of these laws concern groups of health professionals (physicians, dentists, psychotherapists, midwifes, paramedics, etc.) and specify the legal basis for their work. Others govern specific aspects of health care like medical devices, blood or tissue safety, organ transplantation, illegal drugs, etc. Some of the most central legislation in terms of processing health data: • The **Federal Hospitals Act** governs the processing of health data in the inpatient sector. Art. 10 defines the hospitals' obligations for documentation of patient histories. • The **Federal Act on Medical Profession** (Ärztegesetz) 1998, Art. 51, defines independent physicians' obligations for documentation. Art. 51 no. 2 grants treating physicians the right to digitally process personal data related to the patient in treatment as well as to submit the data to specified parties. • The **Telecommunications Act 2003** defines requirements for data security according to GDPR for the providers of communication services. • The **Health Telematics Act 2012** (Gesundheitstelematik-gesetz, HTA 2012) - The second part of the HTA 2012 is the **Federal Act on Data Security Measures when Using Personal Electronic Health Data and Genetic Data** and set in place ELGA, the Austrian national electronic health record scheme, when using personal electronic Health Data, which in turn was enacted by the Electronic Health Record File Act (ELGA Act). - The fourth part of the HTA 2012 deals with ELGA in particular and is restricted to the usage of ELGA Health Data only. Art. 2 no. 9 defines what ELGA Health Data entails. - The HTA 2012 defines Healthcare Providers and the sub-set of the so called ELGA Healthcare Providers as including physicians and dentists (with certain exceptions), hospitals, pharmacies and nursing institutions. Only ELGA Healthcare Providers are allowed and obliged to host ELGA Health Data.The data must be stored in the territory of the European Union. The HTA 2012 also imposes IT security obligations onto institutions hosting and managing data from EHRs.
Legal basis GDPR	• 6(1)(a) consent + 9(2)(a) consent • 6(1)(c) legal obligation + 9(2)(h) provision of health or social care • 6(1)(f) legitimate interest + 9(2)(h) provision of health or social care • Other combination: 6(1)(b) legal obligation + 9(2)(h) provision of health or social care

[36] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Austria. The authors of the report take full responsibility for any interpretations in the country fiche.

	• Other combination: 6(1)(e) public interest + 9(2)(g) substantial public interest on the basis of Union or Member State law
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Art. 10 of the Federal Hospitals Act states that specific regional-level legislation (Landesgesetzgebung) can mandate hospitals to delegate the processing and storage of health data to other legal entities. Transfer of personal health data via a data processor is only possible to physicians, dentists or health care institutions involved in the care of the respective patient. Art. 51 no. 2 of the Act on the Medical Profession (Ärztegesetz) 1998, grants treating physicians the right to digitally process personal data related to the patient in treatment as well as to submit the data to the social insurance bodies and health care providers as far as the recipients' obligations require; as well as, under the condition of the patients consent, to other physicians and health care providers that are treating said patient. Art. 3 no. 4 of the Health Telemactics Act 2012 defines the conditions under which healthcare providers may electronically share health and genetic data: compliance with Art. 9 GDPR; verification of the identity of the individual concerned as well as of the healthcare providers involved in the data exchange; verification of the roles of the healthcare providers; confidentiality and integrity of the data. The Health Telematics Act 2012, in Art. 14, furthermore defines the undirected model of sharing health data implemented by the ELGA EHR infrastructure. Only ELGA Healthcare Providers as defined in Art. 2 no. 10 Health Telematics Act 2012 (see next question for details) are allowed and obliged to host ELGA Health Data. Art. 73 Federal Act on medical devices allows the use of the data for the purpose of protecting the health and safety of patients as and for the purpose of quality assurance of pacemakers.
Legal basis GDPR	• 6(1)(a) consent + 9(2)(a) consent • 6(1)(c) legal obligation + 9(2)(h) provision of health or social care • 6(1)(f) legitimate interest + 9(2)(h) provision of health or social care • Other combination: 6(1)(a) consent + 9(2)(g) substantial public interest on the basis of Union or Member State law • Other combination: 6(1)(e) public interest + 9(2)(g) substantial public interest on the basis of Union or Member State law
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Art. 302 of the Allgemeine Sozialversicherungsgesetz (the law governing the statutory health insurance) provides the legal basis for telerehabilitation, although not specifying provisions related to the processing of health data. Art. 32 and 38 of the Medizinische Strahlenschutzverordnung (decree on radiation protection) specifies under which circumstances teleradiology and teletherapy are allowed, again not addressing data processing. Each telemedicine application including any form of electronic transmission of personal data concerning health by a healthcare provider is subject to the data security requirements as stated in the the second part of the Health Telematics Act 2012. National laws on medical professions do not mention the term "telemedicine" since they are considered as being sufficient for regulating also telemedicine. No legislation but a "soft law" in form of a technical guideline for telemonitoring has been adopted: „Rahmenrichtlinie für die IT-Infrastruktur bei der Anwendung von Telemonitoring: Messdatenerfassung".[37]
Legal basis used for **processing app or device derived data** in the healthcare setting	

[37] See https://www.sozialministerium.at/dam/jcr:c6f54325-0c71-4614-93ff-3358d1cfea27/telemonitoring_rahmenrichtlinie_.pdf

Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent
Specific legislation on **genetic testing**	
National legislation	Austria has specific regulations for genetic testing. Molecular Genetic Testing on humans is regulated by the Federal Gene Technology Act since 1995. Interventions into the inheriting material of the human germ line are prohibited (Art. 64). Genetic tests/analyses for medical purposes (on humans) in Austria are allowed if they follow the state-of-the-art. They are classified into 4 types (Art. 65). This classification is regarding to the potential consequences for the patient, where type 1 has the lowest potential impact. The performance of genetic tests of type 3 and 4 is only allowed in therefore approved facilities and only on the inducement of a medical specialist trained in human genetics/medical genetics or of an attending or diagnosing medical specialist competent for the respective indication. According to Art. 69 a genetic test of type 2, 3 or 4 is only allowed to be performed if there exists a written consent of the person to be tested, that this person has been informed in advance about the nature of the genetic test, the consequences and the significance of the genetic test.

20-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	The **Federal Act on Documentation in Health Care** specifies documentation requirements for the inpatient (Art. 1a-Art. 5c) and the outpatient (Art. 6-Art. 6g) sectors. Acording to Art. 1 the documentation serves the following purposes: • To manage the structure, organization, quality and financing of the Austrian health system • To establish and develop a cross-sectoral quality monitoring system • To ensure cross-sectoral documentation • To implement and monitor the joint health system governance between the federal level, the states and the statutory insurance bodies. As to the inpatient sector, Art. 1a specifies that ICD-10 is the classification used to code diagnoses. Art. 2 specifies the data to be collected per hospital stay. Art. 4 specifies that the Minister responsible for health has to establish a data warehouse 'documentation and information system for analyses in healthcare' with pseudonymised individual level data. Art. 6 specifies the data to be documented in the case of outpatient contacts. ICD-10 classification is not obligatory in the outpatient sector. The same pseudonym has to be used as in the case of the inpatient sector. **The Federal General Social Insurance Act** (ASVG) specifies the data processing regulations in the context of the statutory health insurance (e.g. within its electronic administration system and on the electronic identification card, see Art. 31(a)).
Legal basis GDPR	• 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
Specific legislation addressing 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.	

National legislation	Austria has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Art. 73 and 73a Federal Act on medical devices allows the use of the date that was originally collected for the purpose of providing care for the purpose of protecting the health and safety of patients as well as for the purpose of medical device vigilance and market surveillance and for the purpose of quality assurance of pacemakers, implantable defibrillators and loop recorders.
Legal basis GDPR	• 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 • Other combination: 6(1)(c) legal obligation + 9(2)(j) scientific or historical research purposes or statistical purposes
Specific legislation addressing 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**	
National legislation	Austria has no specific legislation on this topic.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. Art. 4 (15) Federal Epidemics Act, Art. 5 (2) Federal Tuberculosis Act allows for such direct reporting.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	Austria has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
Legislation	In Austria there is no general legal provision for creation of disease registries. Some disease registries have a specific legal basis that regulates its creation and operation, and examples are the Krebsstatistikgesetz and the Epidemiegesetz.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health • Other combination: 6(1)(c) legal obligation + 9(2)(j) statistical purposes in accordance with Article 89(1) • Other combination: 6(1)(e) public interest + 9(2)(j) statistical purposes in accordance with Article 89(1)
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • Public sector researchers • Other national governmental agencies • Other: Public authorities may be given access to the data concerning patients in their coverage. Pseudonymized data may be used by the responsible ministry only for epidemiological surveillance, quality management and to fulfill reporting obligations resulting from EU law. The ministry may authorize a third party for this function.

* Note. 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.

20-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Austria has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Broad consent as defined in national legislation, or in accordance with Recital 33 • Article 9(2)(j) research purposes
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.	Austria has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Broad consent as defined in national legislation, or in accordance with Recital 33 • Article 9(2)(j) research purposes.
National legislation	The legislation does not differentiate between not for profit researchers and for profit researchers. The Federal Research Organisation Act (FOG) regulates the way researchers and research organisations can handle personal data. It is not specific to the health sector, but includes some provisions focused on health data and health research. For both third-party public-sector and not-public-sector researchers, Art. 2(d)(3) FOG applies.

20-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Austria the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Austria:	
Mechanism	• Application to a local research ethics committee • Application to a national data protection agency (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
Art. 7.3 of the Federal Act on the Protection of Personal Data provides guidance on when the approval from the DPA is necessary for the use of data for scientific research purposes. Art. 2(d)(2) FOG specifies that scientific institutions (according to FOG Art. 2(b)(12)) can process personal data for research purposes as long as they are pseudonomyised. Institutions listed in Art. 2(c)(1) or those providing a certificate according to Art. 2(c)(2) can request sector specific pseudonyms provided by the central registry authority (Stammzahlenregisterbehörde), and they can request access to public registers as long as they have been put on a list of available registers by the Minister responsible for research and the Minister under whose purview the register is. In Art. 2(f)(6), the FOG additionally specifies that the Austrian statistical authority (Statistik Austria) can provide data on cause and date of death to research organisations (under certain conditions including confidentiality and an agreement on the purpose of the research). Art. 2(f)(7) then adds that that universities seeking access to data according to Art. 2(f)(6) have to engage university or hospital ethics committees.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Austria did not adopt such a system.	
Legislation has been adopted 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	
Austria has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Austria did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Austria has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
According to the FOG, EHR data in ELGA could be considered register data (Art. 2d(2)(3) FOG). However, according to Art. 38(b) FOG, the responsible Ministers would first have to issue a national regulation adding ELGA to a white list of registers available for secondary use research, which has not been done.	

20-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Austria.

Rights of the patient	How the right can be exercised in Austria
Article 15 'right to access data concerning him or her'	• Through a formal national data access request system established by legislation • Through an access request from the data controller by direct reference to Article 15 GDPR
In the context of the Austrian EHR-system ELGA, a formal national data access request system was established by legislation: Pursuant to Art.16 (1)1. of the HTA 2012, 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). Thus the right to access is restricted according to Art.23(1)(e) GDPR (in conjunction with Art.13(1) HTA 2012 stipulating the substantial public interest in the use of ELGA) in so far as the EHR participants are not entitled to receive this information directly from the controller (i.e. the respective healthcare provider processing their EHR-data).	
Article 16 'right to rectify any inaccurate data concerning him or her'	• 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)
In the context of the Austrian EHR-system ELGA, the right to rectification is restricted according to Art.23(1)(e) GDPR (in conjunction with Art.13(1) HTA 2012 stipulating the substantial public interest in the use of ELGA) under Art.20(1) HTA 2012, pursuant to which already saved EHR-data must not be altered but updated versions have to be saved additionally if circumstances emerge that could cause significant changes in the course of treatment.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	No, a patient may not delete his or her medical record
Due to the minimum retention periods for medical documentation required under Art.51(3) of the Federal Doctors Act 1998 (10 years) and Art.10(1)3. of the Federal Hospitals Act (30 years), the right to erasure does not apply since that processing is necessary for compliance with a legal obligation which requires processing by Member State law to which the controller is subject in accordance with Art.17(3)(b) GDPR. In the context of the Austrian EHR-system ELGA, Art.20(1) HTA 2012 provides that already saved EHR-data must not be altered and therefore not erased. Still, pursuant to Art.16(1)2.(a) HTA 2012 EHR-participants are entitled to set individual access rights by hiding or displaying electronic references and EHR-data or deleting these data. If deleting is prohibited by statutory documentation requirements (such as the minimum retention periods), the electronic references shall be rendered inaccessible for ELGA.	
Article 20 'right to data portability'	Through a formal national data portability request system established by legislation

20-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Austria to include data from apps and devices in the EHR. In addition, the table displays how Austria have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records
There is an ICT system through which patients can access their EHR data
This is organised nationally. Patients can access their personal ELGA records online via the ELGA portal by registering using the Handy-Signatur (digital signature) or Bürgerkarte (electronic identification card). This electronic ID enables the system to verify the patient's unique identity. The ELGA-portal offers citizens the following options:

- View ELGA health data, save it on the computer or print it out
- Inspect the protocol ("who viewed what?")
- See which ELGA-HP currently have access to the own ELGA health data
- Block or unblock discharge summaries or the e-medication list
- Extend or shorten the currently valid access authorizations of your own ELGA-HP
- Exclude individual ELGA-HP from access

Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms

Mechanism	It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs. There are use cases under discussion that allow healthcare professionals to incorporate patient generated data in the context of telemonitoring.

Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'

Austria does not yet participate in eHDSI but plans to do so by 2025.

Technical standards

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

Policy level	• 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)

Within the framework of the ELGA infrastructure, there is a national interoperability policy. ELGA data exchange/storage builds on the HL7 CDA standard. For laboratory data, the LOINC standard is used. For imagine data, a solution with DICOM is in piloting stage. In addition, the ELGA GmbH acts as the national release centre for the SNOMED CT terminology.

In terms of ELGA documents, the so-called "ELGA Interoperability Levels" (EIS) define a certain amount of requirements from CDA Levels 2 and 3. The minimum standards for the data structure of the CDA documents and the dates for the binding use are determined by federal ministerial regulation.

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely

Policy level	There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

Articles 3-8 in the HTA 2012 as well as Articles 17b-k of the ELGA Regulation 2015 lay out the data security framework for the ELGA health record system. There are both technical (encryption, secure networks, etc.) as well as organisational (roles and responsibilities) provisions on data security.

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

Policy level	There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

Articles 14-17a of the ELGA Regulation 2015 lay out the structure, format and standards for health data within the ELGA infrastructure. Article 14, for instance, defines the structure of medication data. Article 16 adds that content, structure, format and coding of ELGA-related health data has to be specified in implementation guidelines (specific guidelines per content type/CDA, building on a general HL7 CDA implementation guideline). Article 17 focuses on terminology (that has to be provided by the Ministry on a terminology server), 17a on temporal availability.

Other relevant provisions in the HTA 2012 include Art. 22 on logging/protocols.

Agencies which oversee the implementation of technical standards

The ELGA governance bodies/owners (Federal Ministry, States, Statutory insurance body) oversee the implementation in terms of ELGA.

21 COUNTRY FICHE POLAND

The following sections provide an overview of the rules for processing of health data currently in place in Poland both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[38]

21-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	In Polish law, after the GDPR came into force, a new law on the protection of personal data was adopted. However, this Act concentrates on formal issues and does not properly contain substantive provisions regarding the processing of health data, such regulations were already enacted before the GDPR became effective. For health prevention purposes processing personal data in healthcare system is based on Art. 3 §2 of the Act on Medical Activity of 15th April 2011 (Dz. U. 2020r. poz. 295**)**, Art. 24 of the Act on Patient Rights and the Patient Ombudsman of 6th November 2008 (Dz.U. 2020., poz. 849). The legal base for processing personal data for purpose of treatment is art. 3 §1 of the Act on Medical Activities and Art. 24 of the Act on Patient Rights and the Patient Ombudsman.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	According to Art. 24 of the Act on Patient Rights and the Patient Ombudsman the data contained in the medical documentation can be processed by persons practicing a medical profession and persons providing ancillary services in the provision of health care. The processing is allowed for protecting health, provision and management of health services, maintaining the ICT system in which medical documentation is processed, and ensuring the security of this system. In accordance with art. 26 §3 of the Act on Patient Rights and the Patient Ombudsman, medical documentation is also made available to entities providing health services if this is necessary for the continuity of health services.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	This is regulated based on the Act on the Information System in Healthcare of 28th April 2011 (Dz. U. 2020 r. poz. 702), in the Minister of Health Regulation on Types, Scope and Models of Medical Documentation and How to Process it of 6th April 2020 (Dz. U. 2020r., poz. 666).
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent

[38] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Poland. The authors of the report take full responsibility for any interpretations in the country fiche.

Specific legislation on **genetic testing**	
National legislation	Poland does not have specific regulations for genetic testing. Work on the adoption of such a law has been underway in Poland for years, although up to the day of this report - no law has been passed. Until the GDPR entered into force, the former Polish Act on the Protection of Personal Data provided that genetic data were particularly sensitive data and subjected to special restrictions. This regulation has been repealed by the new Personal Data Protection Act, which does not contain any regulations in this respect.

21-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	The basis for sharing of health data is Art. 26 of the Act on Patient Rights and the Patient Ombudsman, which contains a list of those entitled to obtain access to medical data. The following public authorities are entitled to such access for the described purposes: • the Patient Rights Ombudsman; • the National Health Fund; • medical self-government bodies and health consultants; • the Patient Rights Ombudsman of the Psychiatric Hospital; • the Agency for Health Technology Assessment and Tariffs; • the Medical Research Agency; • the minister competent for health matters; • entities keeping registers of medical services, to the extent necessary to keep registers; and • persons performing control activities
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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.	
National legislation	Poland has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	This is regulated according to Art. 4 clause 1 point 1 letter g, h, m and n of the Act of 18 March 2011 on the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products (Dz. U. 2020 r., poz. 836), as well as art. 36b of the Pharmaceutical Law of 6th September 2001 (Dz. U. 2020r.poz. 944). The President of the Office for Registration of Medicinal Products, Medical Devices and Biocidal Products has been charged with the following tasks: 1) Collecting and evaluating periodic reports on the safety of medicinal products and collecting information on adverse effects of human or veterinary (investigational) medicinal products, 2) Supervision over the safety of the use of these medicinal products and

	monitoring the safety of their use, 3) Collecting reports of individual adverse reactions from medical practitioners, patients, their legal representatives or actual guardians, as well as information from responsible entities and data from other sources, information from competent authorities of other countries, from specialist literature and obtained as a result of post-authorization safety studies; in the case of biological medicinal products within the meaning of Annex 1 to Directive 2001/83 / EC, information on the name and serial number of those products is collected; 4) Analysis and development of reports, including cause and effect assessment of all reports of individual adverse events; 5) Collecting and analyzing documents regarding the safety of medicinal products; 6) Issuing messages concerning the safety of use of the medicinal product; 7) Agreeing on the content of messages concerning the safety of the medicinal product; 8) Keeping a database of reports of adverse reactions to medicinal products that have occurred in the territory of the Republic of Poland; 9) Forwarding in the EudraVigilance system of individual cases of adverse reactions from the territory of the Republic of Poland to the EudraVigilance database and the central database of the World Health Organization; 10) Cooperation and exchange of information with units that carry out tasks related to poisoning with medicinal products or deal with the treatment of addiction to medicinal products, as well as with relevant authorities; 11) Providing information on medicinal products, including adverse reactions to medicinal products; 12) Taking measures to increase the safety of use of medicinal products; 13) Cooperation with medical practitioners, patients, their legal representatives or actual guardians, in order to ensure effective, correct and reliable reporting of adverse drug reactions of a medicinal product; 14) Immediate forwarding to the European Medicines Agency reports of serious adverse effects of medicinal products; 15) Forwarding to the European Medicines Agency reports of individual cases of adverse reactions 16) Collecting data on the volume of sales of medicinal products in the territory of the Republic of Poland, sent by the responsible entity; 17) Cooperation with other national and international institutions responsible for supervision over the safety of use of medicinal products.
Legal basis GDPR	• Other combination: 6(1)(c) Legal obligation
Specific legislation addressing 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**	
National legislation	This is regulated in the Act of 5 December 2008 on the Prevention and Combating Infection and Infectious Diseases in People (Dz.U. 2020 r., poz. 1845). The act comprehensively regulates the issues of combating infectious diseases and has become the only basis for undertaking violent actions in the field of COVID- 19 in Poland.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. According to art. 29 of the Act on Prevention and Combating Infection and Infectious Diseases in People, laboratory diagnosticians or other persons authorized to carry out laboratory diagnostics on their own, in the case of a test for a biological pathogen in accordance with the provisions issued	

pursuant to paragraph 7 point 1, are obliged in the cases specified in these provisions to report the result of this examination to the competent state sanitary inspector determined in accordance with the provisions issued pursuant to para. 7 point 2. Applications shall be made immediately, but no later than within 24 hours of obtaining the result.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	Identifyiable personal data is not shared. Only access to statistical data published by the entity maintaining the given register is possible. The legal basis are: • The Act of 28 April 2011 on the Information System in Healthcare (Journal of Laws 2011 No. 113 item 657) • Regulation of the Minister of Health of 24 August 2016 on the National Cancer Registry (Journal of Laws 2016 item 1362) • Act of 29 June 1995 on Official Statistics (Journal of Laws 1995 No. 88 item 439) together with the annual regulation on the survey of official statistics.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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

* Note. 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.

21-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Poland has no specific legislation on this topic.
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.	Poland has no specific legislation on this topic.

21-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Poland the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Poland:	
Mechanism	• Application to a local research ethics committee • Application to a national research ethics committee
There are no exemptions.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Poland did not adopt such a system.	
Legislation has been adopted 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	
Poland has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Poland did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Poland has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
There is no specific system to share data for secondary use.	

21-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Poland.

Rights of the patient	**How the right can be exercised in Poland**
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Pursuant to Art. 26 of the Act on Patient Rights and the Patient Ombudsman, the entity providing health services provides medical documentation to the patient or his legal representative, or a person authorized by the patient. Medical records shall be made available: 1) for inspection, including databases in the field of health protection, at the place of providing health services, excluding medical emergency services, or at the seat of the entity providing health services, providing the patient or other authorized bodies or entities with the possibility of taking notes or photos ; 2) by making an extract, copy, copy or printout thereof; 3) by issuing the original with acknowledgment of receipt and subject to return after use, at the request of public authorities or common courts, as well as if a delay in issuing the documentation could endanger the patient's life or health; 4) via electronic means of communication; 5) on an IT data carrier.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16

	GDPR
Poland has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
According to art 29 of the Act on Patient Rights and Patient Ombudsman, medical records are kept for 20 years, from the end of the calendar year in which the last entry was made, except for: 1) medical documentation in the event of the death of a patient as a result of bodily injury or poisoning, which is stored for 30 years from the end of the calendar year in which the death occurred; a. a) medical documentation containing data necessary to monitor the fate of blood and its components, which is stored for a period of 30 years from the end of the calendar year in which the last entry was made; 2) X-ray images stored outside the patient's medical records, which are stored for a period of 10 years from the end of the calendar year in which the photo was taken; 3) referrals for examinations or doctor's orders, which are kept for the period of: a. 5 years from the end of the calendar year in which the health service which was the subject of the referral or doctor's order was provided, b. 2 years from the end of the calendar year in which the referral was issued - in the event that the health service was not provided due to failure to report the patient within the set deadline, unless the patient received the referral; 4) medical records regarding children up to the age of 2, which is kept for a period of 22 years. After the periods specified the entity providing health services destroys medical records in a way that makes it impossible to identify the patient to whom it relates. Medical records intended for destruction may be issued to a patient, his legal representative or a person authorized by the patient. The Act does not give the patient the right to demand its destruction.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

21-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Poland to include data from apps and devices in the EHR. In addition, the table displays how Poland have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
Poland has an online patient account, in which it is possible to access information on medical services, prescriptions but currently there is no medical documentation available on this platform. Running an EHR in Poland is possible on the basis of the Act on the Information System in Healthcare. In practice, however, the system is in the design phase. Currently, patients only have access to payment data for their services, and it is also possible to obtain e-exemptions and e-prescriptions. Access to medical records and their transfer between units is not possible. Each medical unit currently has its own electronic documentation storage system.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so
(Future) Participation in the European infrastructure eHDSI (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Poland is listed among the countries which will implement eHDSI by 2025. Part of the system has already been implemented and the rest is under development. The entire system is to be developed by 2025. According to the Ordinance of the Minister of Health on the e-Health center of June 4, 2020 (Official Journal of the Ministry of Health of 2020, item 42) in Poland, the role of NCPeH is performed by CeZ (e-health center).	

Technical standards

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

Policy level	• 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)

The Ordinance of the Council of Ministers of 12th April 2012 on the National Interoperability Framework sets minimum requirements for public registers and exchange of information in electronic form, and minimum requirements for ICT systems (Dz. U. 2017 r. poz. 2247). In 2017 the Center of Health Information Systems (now e-health center) issued recommendations in the field of security and technological solutions used when processing medical records in electronic form made detailed recommendations taking into account the recommendations of the PN-ISO / IEC 27001 standard. Information technology - Security techniques - Information security management systems, PN-EN ISO 27799 Information technology in health care - Information security management in health care using ISO / IEC 27002.

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

The Ordinance of the Council of Ministers on the National Interoperability Framework sets minimum requirements for public registers and exchange of information in electronic form, and minimum requirements for ICT systems and Recommendations of Center of Health Information Systems (now e-healt center) in the field of security and technological solutions used when processing medical records in electronic form.

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

Policy level	• There is no specific regulation regarding processing medical data for digital applications.

If it is a public data controller, the technical standard is the National Interoperability Framework. The Ordinance of the Council of Ministers on the National Interoperability Framework sets minimum requirements for public registers and exchange of information in electronic form, and minimum requirements for ICT systems and Recomandation of Center of Health Information Systems (now e-healt center) in the field of security and technological solutions used when processing medical records in electronic form.

Agencies which oversee the implementation of technical standards

According to Article 25 of the ACT of 17th February 2015 on IT Activity of Entities Implementing Public Tasks (Dz.U. 2020 r., poz. 346), the Prime Minister (in the implementation of cross-sectoral IT projects), and the Minister of Health (in the implementation of sectoral IT projects) are vested with general powers to control. However, in the case of the operation of ICT systems used for the implementation of public tasks:

a. in local government units and their associations as well as in legal entities and other local government organizational units established or run by these local government units - compliance with the minimum requirements for ICT systems or minimum requirements for public registers and electronic information exchange is performed by the competent voivode

b. in public entities subordinated to or supervised by government administration bodies, compliance with the minimum requirements for ICT systems or minimum requirements for public registers and the exchange of information in electronic form is performed by the government administration body supervising a given public entity,

c, in public entities not listed in point (a) a and b -compliance with the minimum requirements for ICT systems or with the minimum requirements for public registers and electronic information exchange competent is performed by the minister competent for computerization.

21-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	www.bbmri.pl
Hospital and medical specialist care	http://onkologia.org.pl

22 COUNTRY FICHE PORTUGAL

The following sections provide an overview of the rules for processing of health data currently in place in Portugal both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[39]

22-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	Portugal has no specific legislation, however it has several separate laws dealing with the subject: • Lei 58/2019, 08/08/2019 • Lei n.o 12/2005, 26/01/2005 • Decreto-Lei n.o 131/2014, 29/08/2020 • Lei n.o 95/2019, 04/09/2019
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Portugal has no specific legislation, however it has some separate laws dealing with the subject: • Code of Ethics of the Portuguese Medical Association • Lei n.o 81/2009, 21/08/2009 • Decreto-Lei n.o 81/2009, 02/04/2009
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Portugal has no specific law adresssing the general use of health data for digital health services. However there are some provisions in specific information systems to reuse data from other information systems. For example, vaccination information is available at primary care health records through interoperability between different information systems. For app or device generated data, consent is needed as there is no general provision for that.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent
Specific legislation on **genetic testing**	
National legislation	Portugal has specific regulations for genetic testing. It is regulated by Lei n.o 12/2005, 26/01/2005 and Decreto-Lei n.o 131/2014, 29/08/2020.

[39] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Portugal. The authors of the report take full responsibility for any interpretations in the country fiche.

22-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Lei no 81/2008 and Decreto-Lei n.o 82/2009 allow data collection for public health protection by public health authorities.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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.	
National legislation	Portugal has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Portugal has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Lei no 81/2009, 21/08/2009 and Decreto-Lei 82/2009, 02/04/2009 regulate the use of health data for protecting against serious cross-border threats to health.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Portugal has national electronic reporting of laboratory notifications for infectious diseases (national notifiable diseases). Laboratories report by interoperability mechanisms between Lab Information Systems and a central Ministry of Health information system for epidemiologic surveillance. The legislation is Portaria n.º 248/2013, 05/08/2013 ; Portaria n.º 22/2016 ; 10/02/2016.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	There isn´t a general legal provision for creation of disease registries, but there are some disease registries that have a specific legal basis. Examples are: SINAVE: National Epidemiologic Surveillance Information System (Law nº 81/2009) RON: National Oncologic Registry (Law n.º 53/2017).
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • A healthcare professional may be given access to the data that he or she has

	submitted to the registry • A patient may be given access to any data concerning themselves • Other national governmental agencies

* Note. 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.

22-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Portugal has no specific legislation on this topic.
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.	Portugal has no specific legislation on this topic.

22-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Portugal the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Portugal:	
Mechanism	• The data controller provides direct access upon proof of agreement of a research ethics committee or DPA
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Portugal did not adopt such a system.	
Legislation has been adopted 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	
Portugal has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Portugal has adopted a system to facilitate this. At SPMS (Shared Services of Ministry of Health), the National eHealth Agency in Portugal, at 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 who request to data sharing. It manages and oversees the entire process of the request.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Portugal has no specific legislation on this topic.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
There are several national systems to share data for secondary use. Transparency Portal, BI _CSP, and other specific systems share aggregated data for secondary use.

22-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Portugal.

Rights of the patient	How the right can be exercised in Portugal
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
Portugal has not adopted specific legislation on the application of such a right in the area of health.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
Portugal has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

22-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Portugal to include data from apps and devices in the EHR. In addition, the table displays how Portugal have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. Patients can access their EHR data through the electronic health registry in the citizen´s portal of the NHS.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• Healthcare professionals are allowed to incorporate patient generated data into healthcare professional/ provider held EHRs.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Portugal participates in eHDSI through sharing summary records and prescriptions.	
Technical standards	
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	
Policy level	• 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)
Interoperability in health in Portugal is achieved at two levels – technical interoperability and semantic interoperability. It is by combining both resources that secondary use of data is made possible. Given SPMS's status as the National eHealth Agency in Portugal and, given that Health ICT systems are governed by SPMS, **technical interoperability** is achieved via two ways – the setting of policies for connecting to central registries and the usage of two message brokers (one for local, intra institution message exchanges and another for communicating with central databases). This way, information exchanges resorting to these brokers is managed by the usage of the HL7 2.5 and FHIR STU 3 protocols. **Semantic interoperability** is made possible via directives to which all Health ICT systems must comply, published by our National Health Terminologies Center, governed by SPMS and two other Healthcare related national agencies that operate under the Ministry of Health. These directives relate to the usage of "catalogues" for specific purposes, like the registry of allergies related information. Each catalogue is made of a value set, a technical guideline and a functional guideline. Technical guidelines relate to the FHIR service consumption of a catalogue, functional guidelines to how a specific value set should be applied at the point of care and the value set to a subset of a given code system. Value sets available in Portugal are based on the following code systems / terminologies: SNOMED CT, LOINC, ATC, ICD, ICD-10CM/PCS, ICPC-2, TNM, ICNP/CIPE, EDQM and ECDC.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There are several national data security policies which address use of security standards in each healthcare provider sector (primary, secondary, tertiary, long term care)
In Portugal the Government has issued a Specific Resolution, the "Resolution of the Council of Ministers 41/2018", that defines technical guidelines for all Public Administration regarding the security architecture of networks and information systems related to personal data. This document supports the GDPR implementation and describes the technical requirements for front-ends, application layer and database layer, in order to guarantee the securely use and storage of personal data (and sensitive data in the healthcare context) in networks and information systems. Additionally, these guidelines are complemented with internal orientations developed by SPMS, the National Agency for eHealth, namely in the scope of access management, authentication, among others.	
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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.
Agencies which oversee the implementation of technical standards	
SPMS oversees the implementation of technical standards.	

22-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	https://bicsp.min-saude.pt/pt/Paginas/default.aspx
Hospital and medical specialist care	https://benchmarking-acss.min-saude.pt/
Prescription drugs	https://transparencia.sns.gov.pt/explore/?refine.keyword=Medicamentos&sort=modified

23 COUNTRY FICHE ROMANIA

The following sections provide an overview of the rules for processing of health data currently in place in Romania both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[40]

23-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	All applicable legislation provide for the strict confidentiality of patients' medical data and doctor-patient confidentiality. Medical professional secrecy is opposable in Civil Courts, and can only be broken in Criminal investigations under strict conditions. Relevant law includes: • **Law 95/2006** on health care reform, republishing, M.Of. 652 of 28.08.2015 regulates pharmacy, dentistry and organ transplantation. • **Law no. 487/2002** (republished, 11. 07.2002) regulates mental health and protection of persons with mental disorders. • **Order no. 1/2000** (republished) regarding the organization of the activity and the functioning of the forensic medicine institutions • **Law no. 46/2003** on patient rights • **Government Decision 355/2007** for the surveillance of occupational health • Deontological codes of the medical professions • Statute of the occupational health doctors • Various sectorial legislation for epidemiological disease prevention
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Law no. 46/2003 on patient rights, Article 23 states that if the information is required by other accredited healthcare providers involved in the treatment of the patient, consent is no longer required. Law 95/2006 on health care reform, Article 664(1)(c) stipulates that the relationship between healthcare provider and patient may be interrupted "by the doctor, in the following situations: (i) when the patient is referred to another doctor, providing all the medical data obtained, which justifies the assistance of another doctor with enhanced skills". Article 40 of the same law states that (1) The information on the health of persons shall be kept at the territorial public health authorities, at the public health authorities of the ministries with their own health network, as well as at the designated institutions and may be used for the purpose of preparing unnamed statistical reports. of the population. (2) The use for other purposes of the registered information may be allowed only if one of the following conditions is met: a) there is a legal provision in this regard;

[40] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Romania. The authors of the report take full responsibility for any interpretations in the country fiche.

	b) there is the consent of the person concerned; c) the data are necessary for the prevention of the illness of a person or of the community, as the case may be; d) the data are necessary for carrying out the criminal investigation. (3) The maintenance of the confidentiality of the information regarding the persons is obligatory for all the employees who through the activity they carry out have access to them directly or indirectly.
Legal basis GDPR	• 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	There is no specific legislation but only disparate. For example, in the field of telemedicine there are regulations related to telemedicine in rural areas or defense. But there is no regulation that establishes conditions, features, parameters. **Law 95/2006 on health care reform** issues that "Starting with 2018, the rural telemedicine information system and the defense telemedicine information system are part of the health information and information system, public utility projects of national interest, ensuring their implementation and interoperability with other health information and information systems.." **Order of the Ministry of Public Health no. 2021/2008** for the approval of the Methodological Norms for the application of title IV "The national system of emergency medical assistance and qualified first aid" of Law no. 95/2006 on health care reform also mentions the use of telemedicine in first aid. Article 18 states that "Qualified first aid is provided on the basis of protocols and procedures as well as on the basis of remote medical indications, when the telemedicine system is used." Article 22 regulates how and when the telemedicine system may be used for data transmission between ambulances and data reception centres.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	Romania has specific regulations for genetic testing. The Order of the Ministry of Public Health no. **1301/2007** 'for the approval of the Norms regarding the functioning of the medical analysis laboratories' contains very general specifications regarding genetic testing. Specific requirements for the application of SR EN ISO 15189: 2008 in medical analysis laboratories (genetics and molecular diagnosis) are stipulated in '**Medical Laboratories. Special Requirements for Quality and Competence**'. Article 3 of **Law 190/2018** on measures for the implementation the GDPR in Romania sets out special rules for the processing of genetic data, biometric data or health data. • Article 3(1) states that the processing of such data "for the purpose of carrying out an automated decision-making process or for creating profiles, is permitted with the explicit consent of the data subject or if the processing is carried out under express legal provisions, with the establishment of appropriate measures to protect the rights, freedoms and legitimate interests of the data subject." • Article 3(2) states that the processing of health data carried out for the purpose of ensuring public health cannot be performed later, for other purposes, by third parties. With regards to the National Judicial Genetic Data System, **Law 76/2008** 'on the organization and functioning of the National Judicial Genetic Data System' and **Law 118/2019** 'on the Automated National Register on persons who have committed sexual crimes, exploitation of persons or on minors, as well as for the completion of Law no. 76/2008 regarding the organization and functioning of the National Judicial Genetic Data System' apply.

23-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Romania has no specific legislation on this topic. Only for statistics, but not a legal basis under a specific legislation.
Specific legislation addressing 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.	
National legislation	Romania has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Romania has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Romania has no specific legislation on this topic.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. The legal basis is the Government Decision no. 589 of 13 June 2007 on establishing the methodology for reporting and collecting data for the surveillance of communicable diseases.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 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
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	The legal basis for the Romanian Register of Communicable Diseases is the Framework Law on the Organization of the National Institute of Public Health (INSP), according to Law no. 329/2009 and H.G. no. 1,414 / 2009 for the establishment, organization and functioning of INSP, a public institution subordinated to the Ministry of Health.These general regulations are supplemented by: • Government Ordinance no. 53/2000 regarding the obligation to report diseases and perform vaccinations • Government Decision no. 589 of 13 June 2007 on establishing the methodology for reporting and collecting data for the surveillance of communicable diseases • Order of the Ministry of Health no. 1466 of August 20, 2008 for the approval of the information circuit of the single report sheet for communicable diseases

	• Order of the Ministry of Health no. 1101/2016 on the approval of the Norms for surveillance, prevention and limitation of infections associated with health care in health facilities • Order of the Ministry of Health no. 1,829 of October 27, 2020 for approving the information flow used in reporting data on SARS-CoV-2 virus infection, amended by Order no. 1,886 of November 6, 2020
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • A healthcare professional may be given access to the data that he or she has submitted to the registry • 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 • Other national governmental agencies • International agencies such as EMA or ECDC

* Note. 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.

23-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Romania has no specific legislation on this topic.
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.	Romania has no specific legislation on this topic.

23-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Romania the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Romania:	
Mechanism	• Application to a national research ethics committee • 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

No, there is no such entity.
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project
Romania did not adopt such a system.
Legislation has been adopted 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
Romania has no specific legislation on this topic.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
Romania did not adopt such a system.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
There are no provisions in the legislation, it depends on the provision of the contract or agreement.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
The main site of EHR is the following: http://www.des-cnas.ro/pub/ which is not yet functional.

23-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Romania.

Rights of the patient	How the right can be exercised in Romania
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR • Directly, in the electronic health records (EHR). But, at the moment of writing the EHR is not functional
Law mo 95/2006 Art. 3467 stipulates that (1) The access of the patients or of their legal representatives to the data and information from DES is realized in compliance with the provisions of art. 8 of the General Data Protection Regulation, through: a) the security matrix and the access password; b) the national health insurance card with the PIN code associated with it and the access password. However, the EHR (DES) is not functional.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
The right to rectification should be exercised directly, in EHR. However, the EHR (DES) is not functional.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Not clear in legislation
The legislation is not clear on this topic. But based on the provisions of 1) Law 95/2006 regarding the Reform in the field of healthcare, corroborated with 2) Government Decision no. 355/2007 regarding the supervision of occupational health 3) Other legislation in the field of the prevention of certain transmissible diseases 4) And the National Archives Law 16/1996 it can reasonably be concluded that medical records may not be deleted by the health care provider at least for a 100-year period from their creation, both for public interest, and in the best interest of the patient (as such records constitute one's health history that can be useful if not crucial at any later moment in their life, for diagnostic or care provision). **Law 95/2006** on health care reform, Article 346 states that (1) For the patients who expressly refuse the use of the electronic health file, all the existing data in the electronic health file of the patient, constituted under the conditions of art. 3461 para. (3), as well as the data collected after the expressed refusal shall be anonymized, so that the patient cannot be identified in the DES, the	

data being used for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.	
Article 20 'right to data portability'	• 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)
Furthermore, Article 20 GDPR does not apply because data processing is not carried out by automated means (e.g. no Electronic Health record).	

23-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Romania to include data from apps and devices in the EHR. In addition, the table displays how Romania have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. However, it is not operational yet.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Not yet, perhaps in the future. Considering the CNAS "Remarks", it seems so.[41]	
Technical standards	
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	
Policy level	• No, there are no national or regional policies to ensure use of standards for data interoperability
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• No, there are no national or regional data security policies to ensure use of standards for data security
Health data security policies could exist for (some) public institutions.	
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	
Health data quality policies could exist for (some) public institutions.	
Agencies which oversee the implementation of technical standards	
There is no such agency.	

[41] http://www.cnas.ro/post/type/local/precizari-despre-dosarul-electronic-de-sanatate.html

24 COUNTRY FICHE SLOVENIA

The following sections provide an overview of the rules for processing of health data currently in place in Slovenia both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[42]

24-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The processing health data for normal healthcare provision purposes is regulated in the **Healthcare Databases Act** and the **Patients' Rights Act**.
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	The way in which healthcare providers or professionals are allowed to share health data is regulated in the Healthcare Databases Act, the **Health Services Act**, and the **Resolution on the National Health Care Plan** 2016-2025.
Legal basis GDPR	• 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	The Healthcare Databases Act and the Health Services Act, as well as the Resolution on the National Health Care Plan 2016-2025 address the processing of health data for the provision of digital health services. In addition, other relevant legislation is: • **Order determining the types and retention periods of medical documentation** in the Central Register of Patients, • **Rules on authorisations** for data processing in the Central Registry of Patients, **Rules on the prohibition of access** to the patent's data in the Central Register of Patients • **Rules on the referral of patients**, the management of waiting lists, and the maximum permissible waiting times
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) Consent and 9(2)(a) Consent
Specific legislation on **genetic testing**	
National legislation	Slovenia does not have specific regulations for genetic testing. Though there is no specific act, there is an additional **Protocol to the Convention on Human Rights and Biomedicine**, Concerning Biomedical Research in place.

[42] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Slovenia. The authors of the report take full responsibility for any interpretations in the country fiche.

24-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	The Healthcare Databases Act addresses the processing of health data for this purpose.
Legal basis GDPR	• 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
Specific legislation addressing 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.	
National legislation	Slovenia has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	The **Medicinal Products Act** addresses the processing of health data for the purpose of monitoring medical device safety and pharmacovigilance.
Legal basis GDPR	• 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
Specific legislation addressing 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**	
National legislation	This is regulated by the **Communicable Diseases Act**.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. It is regulated by the Healthcare Databases Act and the Communicable Diseases Act.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 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)(i) public interest in the field of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	The Healthcare Databases Act forms the main legal basis and defines the types of registries and sets under what conditions data processing is possible. Annex 1 of the Act defines the content of specific healthcare registries, their purpose, periodic reports, the manner of reporting, and data retention periods.[43]

[43] See also Stanimirovic et al. (2019)

Legal basis GDPR	• 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
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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

* Note. 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.

24-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Slovenia has no specific legislation on this topic.
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.	Slovenia has no specific legislation on this topic.

24-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Slovenia the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Slovenia:	
Mechanism	• The data controller provides direct access without engagement to an ethics committee or DPA
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Slovenia did not adopt such a system.	
Legislation has been adopted 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	
Slovenia has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	

Not known
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Privately funded researchers are not obliged but may choose to do so.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
Each request of researchers for access to data is considered individually in terms of data needs, research objectives, personal data protection, and medical ethics. There is no pre- arranged platform for research purposes as such.

24-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Slovenia.

Rights of the patient	How the right can be exercised in Slovenia
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
In Slovenia, patients' rights are regulated by the Patients' Rights Act.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
In Slovenia, patients' rights are regulated by the Patients' Rights Act.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
In Slovenia, patients' rights are regulated by the Patients' Rights Act.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

24-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Slovenia to include data from apps and devices in the EHR. In addition, the table displays how Slovenia have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records

There is an ICT system through which patients can access their EHR data

This is organised nationally.

The Patient portal zVEM (https://zvem.ezdrav.si) is part of eHealth project. It has more than 765000 visits of the Patient portal zVEM in 2019, around 40000 registered users.

Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms

Mechanism	It is not permitted to incorporate patient generated data into healthcare professional/ provider held EHRs. This functionality is not yet available, and consequently the protocols for the incorporation of patient generated data (by patients or healthcare professionals) are not defined yet.

Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'

Slovenia does not yet participate in eHDSI but plans to do so by 2025.

Technical standards

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

Policy level	• 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)

Slovenia is using a hybrid model , streamlined via a national specific API (adapter) in order to simplify integration of incumbent hospital information systems. The standards are uses as baseline: IHE (xds metadata), HL7 CDA, and OpenEHR – for structured records (such as Patient summary)

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

The National Institute of Public Health has one security policy for the eHealth project which includes EHRs of all Slovenian citizens.

However, each healthcare provider has its own security policy regarding information security of their local ICT systems and related local EHR.

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

Policy level	• There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

There are semantic standards for eHealth services on a national level. Healthcare providers are obliged to follow national coding standards and data models, and there are some validation mechanisms implemented on central platforms.

Examples include: the ePSOS data model for Patient Summary; LOINC –based ontology for document type coding; ICD-10 coding for diseases; ATC coding for medicine substances; SNOMED-CT coding for allergies; and ACHI coding for medical procedures.

However, there are no post processing mechanisms for data quality. It is assumed that healthcare providers are responsible for the quality of submitted data.

Agencies which oversee the implementation of technical standards

The National Institute of Public Health (NIJZ), the Public Health Authority, eHealth Authority Information Commissioner of the Republic of Slovenia and the Data Protection Authority oversee implementation.

24-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	NIJZ Data Portal contains aggregated data https://podatki.nijz.si
Hospital and medical specialist care	

25 COUNTRY FICHE SLOVAKIA

The following sections provide an overview of the rules for processing of health data currently in place in Slovakia both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[44]

25-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The processing health data for normal healthcare provision purposes is regulated by: • Act No. 576/2004 Coll. on **Health Care, Health Care related Services** • Act No. 153/2013 Coll. on **National Health Information System** • Act. No. 18/2018 Coll. on **Personal Data Protection**
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	The way in which healthcare providers or professionals are allowed to share health data is regulated by: • Act No. 576/2004 Coll. on Health Care, Health Care related Services • Act No. 153/2013 Coll. on National Health Information System • Act. No. 18/2018 Coll. on Personal Data Protection
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Based on the Section 45(1)(b) of the Act No. 576/2004 Coll. Ministry of Health adopted **Expert guidance No. 48/2018** and **Expert guidance No. 33/2019** on the usage of specific mobile application by the Emergency Medical Rescue Service Operation Centre, Medical Rescue Service and health care providers for patients with acute myocardial infarction with ST elevation on ECG and with stroke.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) health or social care
Specific legislation on **genetic testing**	
National legislation	Slovakia has specific regulations for genetic testing. The Act. No. 317/2016 Coll. The **Transplantation Act** provides a framework for blood genetic tests for autosome recessive genes in human reproductive cells donors.

25-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used for wider public health purposes

[44] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Slovakia. The authors of the report take full responsibility for any interpretations in the country fiche.

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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Act No. 153/2013 Coll. On National Health Information System addresses the processing of health data for this purpose.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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.	
National legislation	Slovakia has no specific legislation on this topic. Act No. 153/2013 Coll. On National Health Information System only mentions in Section 12 (5) that the National Centre of Health Informatics (operator of the national EHR) cooperates with the Ministry of Health in the area of HTA. No further details are provided in the legislation.
Specific legislation addressing 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**	
National legislation	Slovakia has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	Slovakia has no specific legislation on this topic.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
No, it is not possible.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Slovakia has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	National health registries are health information systems, the primary role of which is to collect, process and analyse data on newly diagnosed diseases occurring on a large-scale or those which are socially significant in the population of the Slovak Republic for the given year (incidence). The total numbers of surviving individuals with diseases monitored in the registries represent prevalence data within a time line. There are also registries for suspected abuse/neglect cases, registry of traumas requiring inpatient care, arthroplasty and assisted reproduction. Access of a third party to the disease registries and the above registries requires consent of the health care provider (or medical professional) who is the source of the data under Section 4 of the Act No. 153/2013 Coll. On National Health Information System. There registries are also basis for statistic comparisons at the international level.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health

Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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. • Other national governmental agencies • Other: Access of a third party to a disease registry requires consent of the health care provider (see above)

* Note. 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.

25-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Slovakia has no specific legislation on this topic.
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.	Slovakia has no specific legislation on this topic.

25-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Slovakia the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Slovakia:	
Mechanism	• Other: Project submission to the National Centre of Health Information
Under the Act. No. 18/2018 Coll. on Personal Data Protection data processing for research purposes is possible. The controller and the processor shall be obliged to accept adequate safeguards for the rights of the data subject. These guarantees shall include the establishment of adequate and effective technical and organizational measures, in particular to ensure compliance with the principles of data minimization and pseudonymisation. The National Centre of Health Information (NCHI) is the Specialised Ministry of Health agency and operates the national EHR system and certain health registries. A researcher may ask NCHI to prepare datasets based on data in the registries operated by NHCI. A project submission is	

necessary in such case. In this case the NCHI usually will require to be a co-researcher. Financing shall be secured for such a project.[45] To our knowledge, there is no mechanism for researchers to access data from EHR.
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project
Slovakia did not adopt such a system.
Legislation has been adopted 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
Slovakia has no specific legislation on this topic.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
Slovakia did not adopt such a system.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Privately funded researchers are not obliged but may choose to do so.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
There is no data access infrastructure entity with the exception of the NCHI operating certain national healthcare related registries and EHR.

25-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Slovakia.

Rights of the patient	How the right can be exercised in Slovakia
Article 15 'right to access data concerning him or her'	• Through a formal national data access request system established by legislation
The patient has, under the provisions of the Act No. 576/2004 Coll on Health Care, Health Care related Services the right to access his or her own medical records and make copies (in the case of hardcopy medical records). It has also the right to access his or her own EHR under the Act No. 153/2013 Coll. On the National Health Information System.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a formal national data rectification request system established by legislation • The right to rectification is restricted based on sectoral legislation adopted in accordance with Article 23(1)
Under Section 5 (3) of Act No. 153/2013 Coll. On National Health Information System, the patient has the right to add own records in his/her patient summary. In the case of an error in medical records only the health care professional who created the record can rectify such record. This applies to both hardcopies (Act No. 576/2004 Coll. on Health Care, Health Care related Services) and EHR (Act No. 153/2013 Coll. On National Health Information System).	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
Act No. 576/2004 Coll. on Health Care, Health Care related Services prescribes how long the medical records shall be stored by the provider – 20 year after last visit (specialists) or 20 years	

[45] See http://www.nczisk.sk/Registre/Narodne-zdravotne-registre/Pages/Pristup-k- udajom-z-narodnych-zdravotnych-registrov-pre-zdravotnickych-pracovnikov.aspx

after the death of the patient (general practitioner). See also Act No. 153/2013 Coll. On National Health Information System.	
Article 20 'right to data portability'	• 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)
Based on the Act No. 576/2004 Coll. on Health Care, Health Care related Services provides no consent of the patient is necessary to processing the personal data during the provision of the health care.	

25-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Slovakia to include data from apps and devices in the EHR. In addition, the table displays how Slovakia have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. In theory any patient having a national ID card with activated authorization function and USB ID card reader can access its own EHR. Persons not having a national ID card, minors aged under 15 and elder citizens having a legacy form of national ID (booklet), are digitally excluded. The location of the specialized portal is https://ezko.npz.sk/. Patients can see e.g. the prescriptions by GP or specialist, and provided inpatient and outpatient care. However, most of the health related data is not included in the EHR.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	Healthcare providers can – in a technical sense – incorporate patient generated data into healthcare professional/ provider held EHRs but in practice hardly ever do so Reasons might be a lack of trust to such data, technical issues with import, legal responsibility for data entered into EHR, etc.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Slovakia is listed among the countries which will implement eHDSI by 2025.	
Technical standards	
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	
Policy level	• 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)
All EHR are placed in a centralized system under the Act No. 153/2013 Coll. On National Health Information System. Interoperability standards for health care informatics are set by the Ministry of Health **Decree No. 107/2015 Coll.** Establishing Standards of Health Care Informatics and Timeframes for the Provision of the Data.	
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely	
Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
Security standards for health care informatics are set by the Ministry of Health Decree No. 107/2015 Coll. Establishing Standards of Health Care Informatics and Timeframes for the Provision of the Data.	
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	
Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.
Agencies which oversee the implementation of technical standards	
The National Centre of Health Information (NCHI) is the Specialised Ministry of Health agency which is inter alia responsible for standardisation of health informatics.	

25-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	National Centre of Health Information http://www.nczisk.sk/en/Pages/default.aspx

26 COUNTRY FICHE FINLAND

The following sections provide an overview of the rules for processing of health data currently in place in Finland both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[46]

26-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	**Act on the Electronic Processing of Client Data in Healthcare and Social Welfare** *[Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)]* The objective of this Act is to promote secure electronic processing of client data in the healthcare and social welfare sector. Electronic client data processing systems and archives shall be established based on this act for the health care. **Act on the Status and Rights of Patients** *[Laki potilaan asemasta ja oikeuksista (785/1992)]* This Act shall apply to the status and rights of patients in health care and medical care unless otherwise provided by statute. **Health Care Act** *[Terveydenhuoltolaki (1326/2010)]* The provisions of this Act shall apply to the implementation and substance of health care services.
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent • 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	The Act on the Status and Rights of Patients and the Health Care Act apply. Patient data sharing is based on patient consent, unless sharing is necessary for treatment of patient and consent may not obtained because of unconsciousness, mental illness or comparable reason. See Act on the Status and Rights of Patients 13 and Act on the Electronic Processing of Client Data in Healthcare and Social Welfare section 10.
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent • 6(1)(c) legal obligation + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Finland has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent • 6(1)(c) legal obligation + 9(2)(h) health or social care • 6(1)(e) public interest + 9(2)(h) health or social care
Specific legislation on **genetic testing**	

[46] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Finland. The authors of the report take full responsibility for any interpretations in the country fiche.

National legislation	Finland does not have specific regulations for genetic testing.

26-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	**Act on the Secondary Use of Health and Social Data** *[Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)]* The purpose of the Act is to facilitate the effective and safe processing and access to the personal social and health data for steering, supervision, research, statistics and development in the health and social sector. A second objective is to guarantee an individual's legitimate expectations as well as their rights and freedoms when processing personal data. **Act on the National Institute for Health and Welfare** *[Laki Terveyden ja hyvinvoinnin laitoksesta (668/2008)]* The purpose of the National Institute for Health and Welfare is to promote health and welfare, prevent diseases and social problems, and to develop social welfare and health care activities and services. The Institute is subordinated to the Ministry of Social Affairs and Health.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation addressing 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.	
National legislation	**Act on the Medical Devices and Supplies** *[Laki terveydenhuollon laitteista ja tarvikkeista (629/2010)]* **Medicines Act** *[Lääkelaki (395/1987)]* The objective of this Act is to maintain and promote the safety of medicinal products and their safe and proper use. A further objective of the Act is to ensure the appropriate manufacture and availability of medicinal products in Finland.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	The Act on the Medical Devices and Supplies has the objective to maintain and promote the safety of medical devices and supplies and their safe and proper use. Also the Medicines Act applies.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation addressing 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**	
National legislation	The **Communicable Diseases Act** *[Tartuntatautilaki (1227/2016)]* has the objective to prevent communicable diseases and their spread, as well as to prevent harmful

	effects caused by these diseases to people and the society.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
Yes, it is possible. A physicians and a dentist must notify the National Institute for Health and Welfare of suspected or diagnosed cases of generally hazardous or monitored communicable diseases, confidentiality provisions notwithstanding. A laboratory carrying out testing for communicable diseases must submit a disease notification of microbial findings on a generally hazardous and monitored communicable disease or other communicable diseases subject to notification, as well as of the sensitivity of microbes to drugs. If the prevention of the spread of a communicable disease requires urgent measures to be performed by a municipality, the person with the obligation to notify must, notwithstanding confidentiality provisions, notify the municipality's physician in charge of communicable diseases of the matter. The person with the obligation to notify must also, notwithstanding confidentiality provisions, notify the municipal health protection authorities of a suspected or discovered epidemic transmitted by drinking water or other environmental sources or by animals, and they must notify the municipal food safety control authorities of an epidemic spreading via foodstuffs. A municipality's physician in charge of communicable diseases must, notwithstanding confidentiality provisions, notify the municipal veterinary authority of a zoonosis he or she either suspects, has diagnosed or has been informed. The Finnish Food Safety Authority must notify the National Institute for Health and Welfare of a suspected or diagnosed animal disease case that may endanger human health. The National Institute for Health and Welfare must notify the Finnish Food Safety Authority of a suspected or diagnosed serious zoonosis that may endanger human health.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	National disease registry data is available for everyone accordingly with the Act on the Secondary Use of Health and Social Data.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(i) public interest in the area of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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 • Other national governmental agencies • Public sector researchers • Private researchers

* Note. 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.

26-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research

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.	Finland has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Broad consent as defined in national legislation, or in accordance with Recital 33 • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes • Other: the legislation does not limit the legal basis, a data controller may decide the basis by themselves.
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.	Finland has specific legislation on this topic. Legal basis: • Explicit Consent (Article 9(2)(a)) • Broad consent as defined in national legislation, or in accordance with Recital 33 • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes • Other: the legislation does not limit the legal basis, a data controller may decide the basis by themselves.

National legislation	In Finland, the legislation does not differentiate between not for profit researchers and for profit researchers. The Act on the Secondary Use of Health and Social Data facilitates the effective and safe processing and access to the personal social and health data for steering, supervision, research, statistics and development in the health and social sector. A second objective is to guarantee an individual's legitimate expectations as well as their rights and freedoms when processing personal data. The Secondary Use Act doesn't regulate the legal basis that should be used. Typically the legal basis is research purposes or consent. Information, including that on customers' well-being, the use of services and costs can be used to support the management of social welfare and health care services. There has previously been no clear legal basis for the collation of data, which is required for knowledge management. Knowledge management is one of the grounds for secondary use of data. Necessary collation of information for the purpose of management from the service provider's own registers is possible without authorization by a permit authority FinData. The Finnish Institute for Health and Welfare has collected data for a long period of time for the national social welfare and health care personal data registers. Previously there have been provisions on these in separate laws. The data in the registers is used for example in national screening and compilation of statistics as well as in research. The legal basis for data collection by the Finnish Institute for Health and Welfare has been made more clear and it is now in accordance with the requirements laid down in the GDPR. From the perspective of social welfare and health care reform, both promoting knowledge management by service providers and the expansion and timeliness of national monitoring data are very important areas of development. Amended legislation will facilitate the better utilization of data to support decision making while respecting the privacy of individuals. The Act on the Secondary Use of Health and Social Data includes provisions on the data permit authority, FinData, its duties, and the secondary use of health and social data. A data permit authority grants data permits when data is needed from numerous different controllers or from the Finnish Institute for Health and Welfare's copy of Kanta data(Kanta service contains most of patient data); and or the data in question is register data from private social welfare and health care service providers. The data permit authority FinData operates at the Finnish Institute for Health and Welfare separate from the institute's other activities. A centralized system for the administration of information requests and data permits

	will be built for communication between the permit authority and the applicant as will secure user environments and user interfaces for the supply of data. This will ensure the better protection of privacy for individuals and the secure use of data.

26-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Finland the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Finland:	
Mechanism	• 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)
There are no exemptions to the principle that the research must first be submitted to the application body.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Finland did not adopt such a system.	
Legislation has been adopted 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	
Finland has no specific legislation on this topic.	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Finland has adopted a system to facilitate this. EHR data is available through the Act on the Secondary Use of Health and Social Data.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Finland has no specific legislation on this topic.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
One infrastructure provided by Findata is preferred, but also other options are available. The Act on the Secondary Use of Health and Social Data states that data with FinData's permission may be processed only in the FinData's secure infrastructure. Another officially approved infrastructure may be allowed if the infrastructure adheres to specifications provided by Findata. It is also possible in some cases, with permission given by single data processors, to utilize another infrastructure.	

26-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Finland.

Rights of the patient	How the right can be exercised in Finland
Article 15 'right to access data concerning him or her'	• Other: Through a formal data access request to the data controllers (health care service providers).

	Patients may also browse their own health data and prescriptions in My Kanta -webpages.
The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare promotes secure electronic processing of client data in the healthcare and social welfare sector. Electronic client data processing systems and archives shall be established based on this act for the health care. The Act on the Status and Rights of Patients applies to the status and rights of patients in health care and medical care unless otherwise provided by statute.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• Through a formal regional data rectification request system established by legislation
The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare and the Act on the Status and Rights of Patients.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare and the Act on the Status and Rights of Patients.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

26-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Finland to include data from apps and devices in the EHR. In addition, the table displays how Finland have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised nationally. Patients can browse their own medical records and prescriptions and order repeat prescriptions via 'My Kanta Pages'.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• 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. Now patients can add limited information to Kanta.fi, but they are developing more features like the possibility to add wellbeing information.
Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
Finland participates in eHDSI through sharing summary records and prescriptions.	
Technical standards	
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	
Policy level	• 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)
There is one national level Kanta-services related policy that defines technical and organizational standards that must be filled to ensure EHR's interoperability with Kanta. Basically EHR interoperability with Kanta is mandatory and required by law. Policies are based on various common health standards like ICD-10, HL7 CDA R2, HL7 Medical	

Records Messages, HL7 FHIR and OAuth 2.0.
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely
Policy level • There are several national data security policies which address use of security standards in each healthcare provider sector (primary, secondary, tertiary, long term care)
Kanta-services policies include data security policies. Also other data security polies especially in the public sector may be applied, like VAHTI information security instructions for government and KATAKRI information security auditing tool for authorities. The Finnish Institute for Health and Welfare (THL) is responsible for the operative guidance of the information management in social welfare and health care. This guidance includes also data security policies for non-Kanta interoperable systems.[47]
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
Policy level • There is one national data quality policy which addresses use of standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)
Kanta-services policies cover also data quality. As for data security policies, the operative guidance of THL includes also data quality policies for non-Kanta interoperable systems.
Agencies which oversee the implementation of technical standards
The National Supervisory Authority for Welfare and Health (Valvira) is the official overseer for the implementation of technical standards. Valvira's statutory purpose is to supervise and provide guidance to healthcare and social services providers. But also Ministry of Social Affairs and Health, Finnish Institute for Health and Welfare, Kela (the Social Insurance Institution of Finland) and the National Cyber Security Centre supervise implemention in their roles.

26-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	THL's Health Care Treatment Register Hilmo https://thl.fi/fi/tilastot-ja-data/aineistot-ja-palvelut/rekisterien-tietosuojailmoitukset/terveydenhuollon-hoitoilmoitukset
Hospital and medical specialist care	HUS Helsinki University Hospital Patient Register https://www.hus.fi/hus-tietoa/hallinto-ja-paatoksenteko/EU-tietosuoja-asetus/Documents/Potilasrekisterin%20informointi%201.1.2020.pdf
Prescription drugs	KELA's Prescription Drugs Registry https://www.kanta.fi/documents/20143/112504/Reseptikeskuksen+Tietosuojaselost e.pdf/87488a6a-697b-3303-7195-2ebc6727cc04

[47] https://thl.fi/en/web/information-management-in-social-welfare-and-health-care

27 COUNTRY FICHE SWEDEN

The following sections provide an overview of the rules for processing of health data currently in place in Sweden both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[48]

27-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	The **Patient Data Act** [Patientdatalag 2008:355] regulates all processing of patient data. All data processing of patient's health care records has to be in accordance with the **Personal Data Act**. For specific purposes, as mandatory care, genetic information etc, there are additional rules, but it has to be based on the Personal Data Act. The Patient Data Act contains ten chapters: 1. Scope. 2. Fundamental rules on processing of personal data. 3. Obligation to keep patient journals. 4. Fundamental rules on secrecy and digital access within a healthcare provider. 5. Fundamental rules on disclosure and obligations to disclose certain information. 6. Coordinated patient overview. 7. National and regional quality registries. 8. Patient rights. 9. Disposals and returns of patient journals. 10. Appeals The general provisions in the Patient Data Act is further elaborated in a regulation issued by the National Board on Health and Welfare: SOSFS 2008:14 National Board of Health and Welfare's **Regulation on Information Processing and Journals Within the Health and Welfare Sector**.
Legal basis GDPR	• 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
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Chapter 4 Section 1 of the Patient Data Act, stipulates that health care professionals are allowed to access documented records about a patient, only if she or he at the time participates in the care of the patient, or if there are other reasons for which she or he needs the data for their work within health care. "Other reasons" refer to situations when health care professionals have an obligation to perform tasks related to quality assessment etc. No other health care professional, even if he or she is employed by the same health care provider, are allowed access to a patient journal. This limitation of access to patient data is called Inner Secrecy [inre sekretess]. Coordinated journals [sammanhållen journalföring] through direct access between different healthcare providers, is regulated in Chapter 6 in the Patient Data Act. In order for a health care professional to process information that another healthcare

[48] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in Sweden. The authors of the report take full responsibility for any interpretations in the country fiche.

	provider has made available through coordinated journals, it is required that 1. The information concerns a patient with whom there is a current patient relationship; 2. The data may be assumed to be important for preventing, investigating or treating illnesses and injuries of the patient in health care, or to coordinate efforts for sick patients and 3. The patient agrees. Every health care provider must ensure that patient data are not accessed by unauthorised health care professionals, and overall make sure that the patient journals are processed in accordance with what is necessary for good and safe health care, see SOSFS 2008:14 Chapter 2 Section 6. Note that the law regarding coordinated journals applies to healthcare providers only. In accordance, it is not possible to provide access for other entities e.g. app- providers or organisations providing other technical services, based on the Patient Data Act.
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent • 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
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	Sweden has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis GDPR	• 6(1)(a) consent and 9(2)(a) consent
Specific legislation on **genetic testing**	
National legislation	Sweden has specific regulations for genetic testing. Chapter 3 section 1 of the Act on Genetic Integrity [Lag (2006:351) om genetisk integritet] states that a genetic test, that constitutes or forms part of a general health examination may only be carried out after permission from the National Board of Health and Welfare. The test may not include anyone other than the person who has given written consent.

27-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	The use of patient data for planning, management, administration and improvement of the health and care systems is also regulated in The Patient Data Act. Chapter 4 section 2 of the Act describes allowed purposes which are: 1. to fulfill the obligations set out in Chapter 3. and prepare other documentation needed in and for the care of patients, 2. administration which concerns patients and which aims to provide care in individual cases or which is otherwise caused by care in individual cases; 3. to draw up any other documentation resulting from law, regulation or other constitution; 4. to systematically and continuously develop and ensure the quality of the business; 5. administration , planning, monitoring, evaluation and supervision of the business; or

	6. to produce statistics on health care. Furthermore, Chapter 7 Sections 4 and 5 contains special provisions on the purposes of processing personal data in national and regional quality registers.
Legal basis GDPR	• 6(1)(c) legal obligation + 9(2)(h) healthcare • 6(1)(e) public interest + 9(2)(h) healthcare
Specific legislation addressing 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.	
National legislation	Sweden has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	The procedures regarding monitoring of medical devise safety and pharmacovigilance are regulated in the **Medicinal Products Act** [Läkemedelslag 2015:315] and the **Medical Products Ordinance** [Läkemedelsförordning 2015:458]. Further procedural regulation has been issued by the Swedish Medical Products Agency [LVFS 2012:14 and LVFS 2012:19] According to Chapter 3 section 13 of the Medical Products Ordinance, The Swedish Medical Products Agency and pharmaceutical companies may process the personal data relating to health that is necessary to fulfill the obligations regarding monitoring of medical devise safety and pharmacovigilance. This includes processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Pharmaceutical companies may however process personal health data for additional purposes, but this requires explicit consent from the patient.
Legal basis GDPR	• Other combination: 6(1)(e) public interest + 9(2)(g) public interest on the basis of Union or Member State law
Specific legislation addressing 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**	
National legislation	This is regulated in the **Act on Protection Against International Threats Against Peoples Health** [lagen (2006:1570) om skydd mot internationella hot mot människors hälsa]. According to section 12, The Public Health Authority [Folkhälsomyndigheten] and other relevant authorities, municipalities and county councils may transfer personal data to the World Health Organization and third countries to fulfill their duties under the law. Information relating to someone's health may be processed, if it's necessary a public authority, a municipality or a county council in order to fulfil the legal obligation to report threats. According to the preparatory works, the authorities must exercise caution when handling patient data, and only share as much as is considered necessary for fulfilling the obligation to notify.
Under MS legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
According to the **Communicable Diseases Act** [Smittskyddslagen 2004:168], section 5, a physician who suspects or detects cases of reportable deceases is obliged to notify this without delay to the medical officer in the county where the notifying physician is working and to the Public Health Authority. The notification must also be made of any other disease that is or is suspected of being contagious, if the disease has received a notable spread within an area or appears in a malicious form. The obligation to notify also applies to a) a physician at a laboratory performing microbiological diagnostics; b) the person responsible for such a laboratory, and c)a doctor performing an autopsy. The Public Health Authority have issued further regulations regarding the obligation to notify, and according to this regulation the obligation to notify cases regarding Covid-19 only applies to the last three groups. See [Folkhälsomyndighetens föreskrifter om anmälan av anmälningspliktig sjukdom i vissa fall HSLF-FS 2015:7].	
Legal basis used for national level specific legislation that has been enacted about other cross-	

border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• Sweden has not adopted specific legislation on this topic
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	The purpose with the access is crucial. Data is only provided for research and statistical purposes. This is regulated in the **Act on Health Data Register** [Lag 1998:543 om hälsodataregister]. According to section 3 and 9, data in such registers may only be processed for the purpose of producing statistics, quality assurance of health care, research and epidemiological investigations. The data is protected in the **Act on Secrecy** [Offentlighets- och sekretesslagen 2009:400], where Chapter 24 section 8 states that personal data may only be made accessible for research and statistical purposes and only if it's clear that it doesn't violate the integrity of the individual or someone close to him or her.
Legal basis GDPR	• 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
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • Other: see the national legislation

* Note. 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.

27-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	Sweden has no specific legislation on this topic.
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.	Sweden has no specific legislation on this topic.

27-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In Sweden the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in Sweden:	
Mechanism	• The data controller provides direct access upon proof of agreement of a research ethics committee or DPA
It is the data controller (the care provider) that provide access, after the decision from the Ethical Review Authority. Direct access requires however that the care provider can assure that this is done in a manner that safeguards other data. If this cannot be guaranteed, the care provider must make the data available by other means.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	
Sweden did not adopt such a system.	
Legislation has been adopted 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	
Sweden has no specific legislation on this topic. The Swedish Research Council (a government agency within the Ministry of Education and Research) has issued a proposal regarding national guidelines on open access to research data. The other main research financers have also acknowledged this stance.[49]	
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes	
Sweden did not adopt such a system.	
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**	
Privately funded researchers are not obliged but may choose to do so.	
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)	
There are several national systems to share data for secondary use. There are more than 100 national disease registries [Nationella kvalitetsregister[50]] in Sweden. They contain individualised patient data concerning diagnosis, medical interventions and outcomes after treatment. The registries are placed at seven regional competence centres, but they are financed jointly the by the state and the Regions. Applications to access the registries must be filed by the competence centre in question.	

27-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in Sweden.

Rights of the patient	How the right can be exercised in Sweden
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
If the data controller is a public care provider, access to health data is guaranteed in accordance with the **The Freedom of the Press Act** [Tryckfrihetsförordningen] and the **Act on Secrecy**. If the data controller is a private care provider, access to health data is regulated in Chapter 8 of the **Patient Data Act**. If the patient is denied access, he or she may appeal the decision to the Administrative Court of	

[49] https://www.vr.se/download/18.2412c5311624176023d25ae1/1556010467675/Forslag-nat-riktlinjer-oppen-tillgang-vetenskaplig%20information_VR_2015.pdf

[50] For a current view, see http://kvalitetsregister.se/englishpages/findaregistry.2027.html

Appeal [Kammarrätt] if it's a public care provider, and the Health and Social Care Inspectorate [Inspektionen för vård och omsorg] if the care provider is private.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16 GDPR
The right of the patient to have incorrect information corrected is solely based on art. 16 GDPR. But according to Chapter 3 Section 8 of the Patient Data Act, the care provider and health care personnel is required to record in the medical record if a patient considers something in the medical record to be incorrect or misleading. The wording of the section shows that this is not a right for the patient, but constructed as an obligation for the care provider and personnel. Accordingly, refusal to record the patient's opinion may not be appealed. Instead, a complaint may be filed with Health and Social Care Inspectorate [Inspektionen för vård och omsorg].	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• Yes, but only under certain conditions
The possibility of having all or part of the medical record destroyed is regulated in Chapter 8 Section 4 of the Patient Data Act. The application should be made to the Health and Social Care Inspectorate. In order for the application to be successful, the following terms apply: 1. The patient must adduce acceptable reasons for the application, 2. It must be obvious that the medical record is not needed for the patient's care in the future, and 3. There are no reasons from the general point of view (e.g. research) to keep the record. The prerequisites mean that the possibility for a patient to have success with an application is very small, and the Health and Social Care Inspectorate seldom grant such applications. The decision of the inspectorate may be appealed to the General Administrative Court, see Chapter 10 Section 2 § of the Patient Data Act.	
Article 20 'right to data portability'	• Patients cannot obtain a portable copy of medical records
Article 20 GDPR does not apply because health data are not collected on the basis of consent and no sectoral legislation allows this.	

27-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in Sweden to include data from apps and devices in the EHR. In addition, the table displays how Sweden have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
• This is organised nationally. • This is organised regionally. The platforms governed by Inera are used for different aims. For example, the NPÖ uses the same connections as the Medical Records [Journalen], where patients may access their medical records on-line, as far as they have been made available by the care providers. Journalen is part of the Care guide 1177 [Vårdguiden 1177, 1177.se]. All of the Regions have entered the Medical Records, but the patient data provided for the patient is similar to the data accessible through NPÖ, described above. Furthermore, some data are considered more sensitive, e.g. psychiatric care, and not shared by all Regions through the Medical Records. Besides the Medical Records, some Regions also offer local digital services, mainly in the area of primary care. These services may include counselling, documentation of medical background, digital examinations and triage.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• 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 Several Regions plan for or have initiated pilot project to test digital products or services for patients with cronic disease, as chronic obstructive lung disease and heart failure. To some extent services like these has also been implemented, in cooperation with private interests. The Swedish Association of Local Authorities and Regions [Sveriges kommuner och regioner, SKR] have called for a national recommendations regarding financing of the services, issues regarding the legal basis and data security, the need for a national infrastructure.[51]

Participation in the European infrastructure **eHDSI** (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'

Sweden does not yet participate in eHDSI but plans to do so by 2025.

The Swedish e-Health Agency is the national contact point for cross-border health care and analysed the situation regarding transfer of patient data last year, on behalf of the government. The Agency concluded that the legal conditions for participation need to be investigated further. The Agency also called for further analysis on how the consent of the patient best could be handled, if the right to integrity is to be adequately safeguarded.[52]

Technical standards

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

Policy level	• 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)

The policy is currently a work in progress. Inera have initiated a project called Safe Digital information [Säker digital information, SDK, https://inera.atlassian.net/wiki/spaces/OISDK/overview?homepageId=4032938

]. The Swedish Association of Local Authorities and Regions as well as the Agency for Digital Government [Myndigheten för digital förvaltning, DIGG] are among the many participators in the project. SDI builds upon the experiences by the Connecting Europe Facility (CEF) eDelivery, and the standardisation project is intended to finish in 2022.

The aim of the project is to construct a standard that makes it possible to transfer sensitive data in a unified, efficient and secure manner.

Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely

Policy level	• There is one national data security policy which addresses use of security standards across all healthcare provider sectors (primary, secondary, tertiary, long term care)

According to the guidelines on information processing and journals from the National Board on Health and Welfare (HSLF-FS 2016:40), the care providers are encouraged to use Swedish standards in the ISO/IEC 27000-series.

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

Policy level	• No, there are no national or regional policies to ensure use of quality standards for health data.

There are standards from the National Board on Health and Welfare regarding the terminology used in the medical documentation, but no standards regarding the technical quality.

Agencies which oversee the implementation of technical standards

In december 2020, The Agency for Digital Government [Myndigheten för digital förvaltning, DIGG] was entrusted with the task to lead and coordinate the public authories' work to construct a united digital infrastructure for data exchange and facilitate increased digitalization and uniform digital solutions in the social sector.

[51] See Sveriges kommuner och regioner, Ordnat införande https://skr.se/halsasjukvard/ehalsa/standardiseringinformatik/ordnatinforandedigit alatjanster.15226.html

[52] See eHälsomyndigheten, Informationshantering vid utlandsvård, https://www.ehalsomyndigheten.se/globalassets/dokument/rapporter/information shantering-vid-utlandsvard_final.pdf

27-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Self measurements	The organisation of the quality registries seems to work fine, with regards to access for researchers. https://kvalitetsregister.se/englishpages/useregistrydatainyourresearch/guidanceondisclosureofregistrydata.2410.html

28 COUNTRY FICHE UNITED KINGDOM

The following sections provide an overview of the rules for processing of health data currently in place in the United Kingdom both in terms of legislative measures as well as the practical and technical manner in which health data is governed at national level.[53] Note that the United Kingdom has become a third country to the European Union since 31 December 2020, the impact of which on the cross-border sharing of data is beyond the scope of this study and country fiche.

28-1 Function 1 (primary use for provision of health and social care by health and care providers to the patient concerned)

First we address the area of 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.

Processing health data for the primary use of providing health and social care	
Legislation on **processing health data for normal healthcare provision** purposes within the context of a patient - healthcare professional relationship	
National legislation	In England, all health and adult social care providers are subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about a patient for their direct care. This duty is subject to both the common law duty of confidence and the UK's Data Protection Act 2018 and the GDPR. The legal basis of Art 6(1)(e) does not need to refer specifically to the processing of personal data but must establish the 'official authority' to conduct the activity for which the processing is necessary. Some examples are: NHS England: NHS Act 2006; Clinical Commissioning Groups: NHS Act 2006; NHS Digital: Health and Social Care Act 2012; GP Practices: NHS England's powers to commission health services under the NHS Act 2006 or to delegate such powers to CCGs; NHS Trusts: National Health Service and Community Care Act 1990; NHS Foundation Trusts: Health and Social Care (Community Health and Standards) Act 2003; Local authorities: Local Government Act 1974, Children Act 1989, Children Act 2004, and Care Act 2014.
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(h) provision of health or social care
Legislation that regulates the way in which **healthcare providers or professionals are allowed to share health data** with another healthcare provider or healthcare professional for healthcare provision purposes	
National legislation	Health and Social Care Act 2012 (England) Section 259 gives the Health and Social Care Information Centre (now known as NHS Digital) the power to require providers of health and social care in England to send it confidential data in limited circumstances, including when directed to do so by the UK Secretary of State for Health or NHS England. Patient consent is not needed, but patient objections will be handled in line with the pledges set out in the NHS Constitution for England and directions given to NHS Digital by the Secretary of State. Statutory restrictions on disclosing information about patients are the Gender Recognition Act 2004 (UK) and Human Fertilisation and Embryology Act 1990 (UK).
Legal basis GDPR	• 6(1)(e) public interest + 9(2)(h) provision of health or social care
Specific law addressing the processing of health data **for providing digital health services**	
National legislation	The United Kingdom has no specific legislation on this topic.
Legal basis used for **processing app or device derived data** in the healthcare setting	
Legal basis	• 6(1)(e) public interest + 9(2)(h) health or social care

[53] Acknowledgement: this country fiche is assembled based on the response on the legal survey from the national country correspondents in the United Kingdom. The authors of the report take full responsibility for any interpretations in the country fiche.

GDPR	
Specific legislation on **genetic testing**	
National legislation	The United Kingdom does not have specific regulations for genetic testing.

28-2 Function 2 (secondary use for planning, management health systems improvement)

Function 2 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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 device.

Processing health data for the secondary use of planning, management and improvement of the healthcare system	
Specific legislation addressing the processing of health data for **planning, management, administration and improvement of the health and care systems entities** such as health authorities	
National legislation	Northern Ireland: Health and Social Care (Control of Data Processing) Act 2016 requires the Department of Health in Northern Ireland to make regulations that permit or require the processing of confidential information for defined health and social care purposes. The Act does not set aside the Data Protection Act 2018 or the Human Rights Act 1998 and any use of information must continue to comply with the requirements of these two pieces of legislation. England and Wales: Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. The person responsible for the information must still comply with all other relevant legal obligations such as the Data Protection Act 2018 and the Human Rights Act 1998. The regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Section 259 of the Health and Social Care Act 2012 (England) gives the Health and Social Care Information Centre (known as NHS Digital) the power to require providers of health and social care in England to send it confidential data in limited circumstances, including when directed to do so by the UK Secretary of State for Health or NHS England.
Legal basis GDPR	• 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
Specific legislation addressing 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.	
National legislation	The United Kingdom has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	The United Kingdom has no specific legislation on this topic.
Specific legislation addressing 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**	
National legislation	• The Health Protection (Notification) Regulations 2010 • The Health Protection (Notification) (Wales) Regulations 2010 • Public Health etc. (Scotland) Act 2008 • Public Health Act (Northern Ireland) 1967 • The Health Service (Control of Patient Information) Regulations 2002 – specifically

	Regulation 3 In March 2020, the Secretary of State for Health issued a notice under Regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) to require organisations to process confidential patient information for purposes set out in Regulation 3(1) of COPI. The Notice requires organisations to process confidential patient information for the purposes set out in Regulation 3(1) of COPI to support the Secretary of State's response to Covid-19 (Covid-19 Purpose). "Processing" for these purposes is defined in Regulation 3(2) and includes dissemination of confidential patient information to persons and organisations permitted to process confidential patient information under Regulation 3(3) of COPI.
Under national legislation, is it possible that data are transmitted **from the laboratories directly to institutions dealing with communicable diseases/ECDC**, without going through a reporting cascade, and if so, what is the legislation or guidance that allows for such direct reporting?	
No, it is not possible.	
Legal basis used for national level specific legislation that has been enacted about other cross-border health threats, such as food borne diseases, sexually transmitted diseases, **which are not covered by the WHO International Health Regulation***	
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Specific legislation has been enacted to address **the creation of disease registries** (which can be used to record the prevalence and incidence of certain diseases, both common and rare)	
National legislation	Under Regulation 2 of The Health Service (Control of Patient Information) Regulations 2002 (as part of section 251 of the NHS Act 2006), the processing of confidential patient information for the purposes in connection with the construction and maintenance of cancer registries may be undertaken by bodies or persons who (either individually or as members of a class) are approved by the Secretary of State, and authorized by the person who lawfully holds the information. The legislation itself does not specify categories of people who may legally be given access to data held in the disease registry.
Legal basis GDPR	• 6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health • 6(1)(e) public interest + 9(2)(i) public interest in the field of public health
Access	According to the legislation the following actors may legally be given access to data held in the disease registry: • 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

* Note. 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.

28-3 Function 3 (secondary use for scientific or historical research by both public and private sector organisations)

Function 3 concerns the re-use of health data that were collected initially in the context of providing care, but which may later be re-used 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.

Processing health data for the secondary use of scientific or historical research	
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.	the United Kingdom has no specific legislation on this topic.
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.	the United Kingdom has no specific legislation on this topic. Legal basis: • Article 9(2)(i) public interest in the field of public health • Article 9(2)(j) research purposes
National legislation	In the United Kingdom, the legislation does differentiate between not for profit researchers and for profit researchers. Section 122 of the Care Act 2014 amends the Health and Social Care Act 2012 (section 261 1A) to provide that NHS Digital may only disseminate information under its general dissemination power in section 261(1) for the purposes of the provision of health care or adult social care or for the promotion of health. This would enable data to be made available for a wide range of health and care related purposes – including for the commissioning of those services, and the epidemiological research that is needed at the earlier stages of developing new treatments – *but not for solely commercial purposes such as for commercial insurance.*

28-4 Legal or regulatory mechanisms which address the use of health data for research purposes

Access to health data for research can be organised in various manners. In the United Kingdom the following list of forms is used, not excluding other forms that may exist, e.g. at regional level.

Legal or regulatory mechanisms for Function 3	
Mechanisms through which **access to health data for research** is organised in the United Kingdom:	
Mechanism	• Application to a local research ethics committee • 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)
Whether data is anonymous or pseudonymous or fully identifiable, it is expected that an application will be made to a NHS Research Ethics Committee. Depending on the data identifiability, a different approach to the review will take place (i.e. full committee review versus proportionate review). Exceptions are made for Research Ethics Committee review when: • Research is limited to secondary use of information previously collected in the course of normal care (without an intention to use it for research at the time of collection) provided that the patients or service users are not identifiable to the research team in carrying out the research. • Research is undertaken by staff within a care team using information previously collected in the course of care for their own patients or clients, provided that data is anonymised in conducting the research. Research involves information which has been anonymised by an intermediary before its onward release to the researchers provided that there is a legal basis for the anonymisation.	
A **data altruism system** has been adopted that establishes a possibility for patients to provide their data to be used by researchers without reference to a particular research project	

In the United Kingdom, a data altruism system has been created at regional level. In the UK, there is mostly a presumption that health data – and specifically confidential patient data – will be used for research (and planning) purposes, rather than a presumption that it won't. In England, the national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes. Scotland has a separate opt-out, offered through the Scottish Primary Care Information Resource (Spire). 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.
Legislation has been adopted 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
The United Kingdom has no specific legislation on this topic. However, the federated institute Health Data Research (HDR UK) requires that all participating organisations make data FAIR by adopting the FAIR Guiding principles for scientific data management and stewardship.
A system has been adopted to facilitate the **re-use of electronic health record data** for research purposes
the United Kingdom has adopted a system to facilitate this. The HDR UK can be viewed as a kind of 'system' to facilitate re-use of EHR data for research purposes. Also, NHS Digital provides Clinical Records Standards, which provide a consistent way of collecting information for the NHS and providing the service to enable clinical data sets to be analysed.
Legislation has been adopted which requires privately funded researchers to **share the research data with public bodies**
Privately funded researchers are not obliged but may choose to do so. There is no legislation per se. However, in early 2020, NHS Digital and the Private Healthcare Information Network (PHIN) launched a consultation and a series of trials around the integration of private healthcare data and NHS recorded activity. Under the Acute Data Alignment Programme (ADAPt) launched in 2018, PHIN will share private healthcare data with NHS Digital, creating a single source of healthcare data in England. The central dataset is intended to allow providers, care planners, regulators and researchers to better understand how private and public healthcare data sits alongside each other and how it can be used to improve care overall.
Data access infrastructure entities through which researchers can share, and access EHR data for research purposes (function 2 or function 3)
There are several sector specific regional systems to share data for secondary use. Different regional systems exist across the UK. Two examples are the Secondary Uses Service, ran by NHS Digital in England, and the Health Data Research Innovation Gateway, ran by HDR UK.

28-5 Patients' 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. The table displays how those rights can be exercised in the context of health-related data in the United Kingdom.

Rights of the patient	How the right can be exercised in the United Kingdom
Article 15 'right to access data concerning him or her'	• A patient needs to request access from the data controller by direct reference to Article 15 GDPR
The United Kingdom has not adopted specific legislation on the application of such a right in the area of health.	
Article 16 'right to rectify any inaccurate data concerning him or her'	• A patient needs to request rectification from the data controller by direct reference to Article 16

	GDPR
The United Kingdom has not adopted specific legislation on the application of such a right in the area of health.	
Article 17 'right to be forgotten' May a patient have medical records deleted?	• No, a patient may not delete his or her medical record
The United Kingdom has not adopted specific legislation on the application of such a right in the area of health.	
Article 20 'right to data portability'	• A patient needs to request portable data from the data controller by direct reference to Article 20 GDPR

28-6 Electronic Health Records and technical standards

Electronic Health Records (EHRs) are a core building block of electronic data collection, processing and sharing. The table shows which mechanisms are used in the United Kingdom to include data from apps and devices in the EHR. In addition, the table displays how the United Kingdom have adopted policies, guidelines or legal requirements that ensure technical standards on interoperability, security and quality are used by healthcare provider organisations.

Electronic Health Records	
There is an ICT system through which patients can access their EHR data	
This is organised by individual health services. The EHR market in the UK is currently dominated by a few large suppliers. The majority of software for Summary Care Records and GP practices is provided by EMIS, TPP and inPractice. Large suppliers of hospital software include Cerner, CSC, BT and IMS Maxims. Open Source software is also increasingly used, and has been endorsed by NHS England. The Care Quality Commission has identified cases where IT systems from different suppliers do not communicate effectively, with staff consequently reverting to using paper records. The NHS, local authorities, clinical staff and software providers have committed to ensuring that electronic health records are interoperable, but this commitment has been met in practice.	
Citizens increasingly use **apps and devices** to track and record issues like food intake, exercise, sleep etc. Such data may be included into EHRs through the following mechanisms	
Mechanism	• 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
Participation in the European infrastructure eHDSI (eHealth Digital Service Infrastructure), also known as 'MyHealth @ EU'	
The United Kingdom does not (plan to) participate in such European infrastructures.	
Technical standards	
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	
Policy level	• 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)
In general, interoperability across the UK is lacking. Each region has its own interoperability policies and vary depending on the healthcare provider sectors. Discussions have taken place between NHS England and the Welsh for an interoperability policy. The HSCIC in Northern Ireland has published an 'Interoperability Handbook' to outline common specifications, frameworks and standards for medical software and accredits systems which meet them. NHS Trusts are advised to take this into account during procurement, but this is not a legal requirement. In England, the Chief Clinical Information Officer for health and care in England has outlined seven priority areas for interoperability. SNOMED CT must be utilised in place of Read codes before 1 April 2018 across Primary care settings. For Secondary Care, Acute Care, Mental Health, Community systems, Dentistry and other systems used in the direct management of care of an individual must use SNOMED CT as the clinical terminology before 1 April 2020. NHS Digital (in England) has also advocated that all NHS digital, data and technology services should support Fast	

Healthcare Interoperability Resources (FHIR)-based APIs to enable the delivery of seamless care across organisational boundaries.
Health data security policies regarding the technical standards to be used to ensure health data for primary use are processed and stored securely
Policy level • Each region has several data security policies which address use of security standards in each healthcare provider sectors (primary, secondary, tertiary, long term care)
In England, the National Data Guardian's (NDG) Data Security Standards are intended to apply to every organisation handling health and social care data, although the way that they apply will vary according to the type and size of organisation. In the other nations, there are a mix of health data security standards, generally organised by healthcare provider sectors (e.g. for healthcare: NHS Scotland, NHS Wales and HSC Northern Ireland).
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
Policy level • Each region has several data quality policies which address use of standards for each healthcare provider sectors (primary, secondary, tertiary, long term care)
Data quality policies vary by region and healthcare provider sector. For example, NHS England has published 'Data Quality: Guidance for providers and Commissioners' and NHS Wales has published a 'Data Quality Policy'. NHS National Services Scotland runs 'data quality exercises' to ensure the Community Health Index (CHI) are current with patient demographic details, as well as registration status. Public Health Scotland has a Data Quality Assurance (DQA) Team to advise and assess the quality of Scottish Morbidity Record data submitted to national databases.
Agencies which oversee the implementation of technical standards
National Data Guardian for Health and Social Care, NHS England, NHS Scotland, NHS Wales and HSC Northern Ireland, Public Health England, Public Health Scotland, Public Health Wales.

28-7 National examples of organisations and registries on secondary use of health data

Purpose of processing	National example
Primary care data	NHS Digital https://digital.nhs.uk/data-and-information/areas-of-interest/primary-care
Hospital and medical specialist care	NHS Digital https://digital.nhs.uk/data-and-information/areas-of-interest/hospital-carehttps://digital.nhs.uk/data-and-information/areas-of-interest/hospital-care
Prescription drugs	NHS Digital https://digital.nhs.uk/data-and-information/areas-of-interest/prescribing
Self measurements	NHS Digital https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/patient-reported-outcome-measures-proms

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-01-21-048-EN-N

ISBN 978-92-9478-786-6