



Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

Written by Francisco Lupiáñez-Villanueva, Laura Gunderson, Simone Vitiello, Nuria Febrer, Frans Folkvord, Loic Chabanier, Nihal Filali, Raphaël Hamonic, Eline Achard, Hélène Couret, Maria Teresa Arredondo, Maria Fernanda Cabrera, Rebeca García, Laura López, Beatriz Merino, Giuseppe Fico

July/2021



EUROPEAN COMMISSION

Directorate-General for Health and Food Safety

Directorate B — Health systems, medical products and innovation

Unit B3 — Digital Health, European Reference Networks

Contact: Yiannos Tolias

E-mail: Yiannos.TOLIAS@ec.europa.eu/sante-consult-b3@ec.europa.eu (functional mailbox)

*European Commission
B-1049 Brussels*

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

Directorate-General for Health and Food Safety

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (<http://www.europa.eu>).

PDF ISBN: 978-92-76-47023-6

doi: 10.2875/702007

EW-01-22-062-EN-N

Manuscript completed in July/2021

Luxembourg: Publications Office of the European Union, 2022

© European Union, 2022



The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

Table of Contents

ABSTRACT.....	12
EXECUTIVE SUMMARY.....	13
1. BACKGROUND AND METHODOLOGY	16
1.1 CONTEXT OF THE STUDY	16
1.2 OBJECTIVES AND SCOPE.....	16
1.2.1 <i>Digital health products and services</i>	17
1.2.2 <i>Artificial intelligence in health</i>	17
1.2.3 <i>Governing the use of health data</i>	18
1.2.4 <i>Evaluation of Article 14 of Directive 2011/24/EU</i>	19
1.3 METHODOLOGICAL APPROACH	21
1.3.1 <i>Scoping review and desk research</i>	22
1.3.2 <i>Stakeholders' consultations</i>	22
1.3.3 <i>Analysis and triangulation</i>	25
1.4 LIMITATIONS OF THE STUDY.....	26
2. DIGITAL HEALTH PRODUCTS AND SERVICES	27
2.1 SCOPING THE FIELD	27
2.1.1 <i>Definitions</i>	27
2.1.2 <i>Overview of the provision of digital health services and products on the market</i>	31
2.1.3 <i>Current EU MS national practices and cross-border provision</i>	33
2.2 FOSTERING CROSS-BORDER DIGITAL HEALTH: DRIVERS, OBSTACLES, COSTS AND BENEFITS	36
2.2.1 <i>Background</i>	36
2.2.2 <i>Approval, certification, authorisation and reimbursement</i>	37
2.2.3 <i>Interoperability</i>	51
2.2.4 <i>Data protection and liability</i>	60
2.2.5 <i>Professional qualifications</i>	67
2.2.6 <i>Online sales of pharmaceutical products</i>	71
2.3 CURRENT REGULATORY PRACTICES AND GAPS	73
2.3.1 <i>Member State approaches</i>	73
2.3.2 <i>Existing EU-level initiatives</i>	80
2.3.3 <i>Implementing a European Medical Devices legal framework</i>	80
2.3.4 <i>Legislative Inhibitors</i>	84
3. ARTIFICIAL INTELLIGENCE IN HEALTH	86
3.1 SCOPING THE FIELD	86
3.1.1 <i>Definitions and techniques</i>	86
3.1.2 <i>Areas of AI use and levels of control in healthcare</i>	89
3.1.3 <i>AI development and implementation</i>	95
3.1.4 <i>AI performance and economic impact</i>	97
3.1.5 <i>Challenges of AI use in healthcare</i>	103
3.2 REGULATORY LANDSCAPE AND GAPS	108
3.2.1 <i>Current EU framework</i>	108
3.2.2 <i>Examples from Canada, US and UK</i>	114
3.2.3 <i>Current gaps</i>	118
3.2.4 <i>The new EU proposals</i>	141
4. GOVERNING THE USE OF HEALTH DATA.....	147

4.1 SCOPING THE FIELD	147
4.1.1 <i>Analysing the value of health data</i>	147
4.1.2 <i>Health data exchange for healthcare provision (primary purposes)</i>	162
4.1.3 <i>Health data access for research, innovation, policy-making and regulatory decision (secondary purposes)</i>	170
4.2 REGULATORY LANDSCAPE	185
4.2.1 <i>Health data exchange for healthcare provision (primary purposes)</i>	185
4.2.2 <i>Health data access for research, innovation, policy making and regulatory decision (secondary purposes)</i>	
	192
5. EVALUATION OF ARTICLE 14 OF DIRECTIVE 2011/24/EU	197
5.1 DESCRIPTION OF THE INITIATIVE AND ITS OBJECTIVES	197
5.2 BASELINE	201
5.3 IMPLEMENTATION STATE OF PLAY.....	202
5.3.1 <i>Input</i>	202
5.3.2 <i>Activities</i>	204
5.3.3 <i>Outputs</i>	208
5.3.4 <i>Outcomes</i>	208
5.3.5 <i>Impacts</i>	213
5.3.6 <i>Other EU policies</i>	218
5.3.7 <i>Member States digitalisation and interoperability and the impact of the eHealth Network</i>	221
5.4 ANALYSIS AND EVALUATION	225
5.4.1 <i>Effectiveness</i>	225
5.4.2 <i>Efficiency</i>	227
5.4.3 <i>Relevance</i>	233
5.4.4 <i>Coherence</i>	234
5.4.5 <i>EU added value</i>	236
6. CONCLUSIONS AND RECOMMENDATIONS	239
6.1 DIGITAL HEALTH PRODUCTS AND SERVICES	239
6.1.1 <i>Establish labelling/certification/authorisation guidance for digital health services and products</i>	239
6.1.2 <i>Define the scope of telehealth/mHealth products and services to be reimbursed</i>	242
6.1.3 <i>Facilitate the use of digital products/services and the access to patients' data</i>	243
6.1.4 <i>Ensure transparency of digital health services and products provided cross-borders</i>	245
6.1.5 <i>Ensure an appropriate liability framing for digital health</i>	246
6.2 ARTIFICIAL INTELLIGENCE IN HEALTH	247
6.3 GOVERNING THE USE OF HEALTH DATA.....	253
6.3.1 <i>European Health Data Space</i>	253
6.3.2 <i>Policy options for primary use</i>	254
6.3.3 <i>Policy options for secondary use</i>	255
6.4 EVALUATION OF ARTICLE 14 OF DIRECTIVE 2011/24/EU	256
7. REFERENCES	262
8. ANNEX	279
8.1 RESEARCH QUESTIONS	279
8.1.1 <i>Digital health products and services</i>	279
8.1.2 <i>Artificial intelligence in healthcare</i>	281
8.1.3 <i>Governing the use of health data</i>	284
8.1.4 <i>Evaluation of Article 14 of Directive 2011/24/EU</i>	284
8.2 SEARCH STRINGS AND PRISMA DIAGRAMS.....	287

8.2.1	<i>Digital health products and services</i>	287
8.2.2	<i>Artificial intelligence in healthcare</i>	288
8.2.3	<i>Governing the use of health data</i>	289
8.2.4	<i>Evaluation of Article 14 of Directive 2011/24/EU</i>	291
8.3	OVERVIEW OF THE CONSULTATION PHASE	293
8.3.1	<i>In-depth interviews</i>	293
8.3.2	<i>Workshops</i>	295
8.3.3	<i>Online questionnaires</i>	299
8.4	DIGITAL HEALTH PRODUCTS AND SERVICES	300
8.4.1	<i>eHealth scope</i>	300
8.4.2	<i>ePrescription</i>	300
8.4.3	<i>Main medical standards (Schultz et al., 2019)</i>	301
8.4.4	<i>Focus areas of the Interoperability action plan</i>	303
8.4.5	<i>Draft Code of Conduct practical guidelines for app developers</i>	303
8.5	GOVERNING THE USE OF HEALTH DATA.....	305
8.5.1	<i>Calculating value of health data</i>	305
8.5.2	<i>Estimated economic value of health data</i>	308
8.5.3	<i>Cost of cybersecurity breaches</i>	316
8.6	EVALUATION OF ARTICLE 14 OF DIRECTIVE 2011/24/EU	319
8.6.1	<i>Evaluation matrix</i>	319
8.6.2	<i>Potential future financial inputs</i>	325
8.6.3	<i>Multiannual Work Plan activities and outputs</i>	327
8.6.4	<i>Future activities</i>	334
8.6.5	<i>Examples of European funded projects in eHealth</i>	336

List of Tables

Table 1. Summary table of consultation phase and desk research	23
Table 2. Overview of definitions.....	32
Table 3. Approval, certification, authorisation and reimbursement drivers.....	50
Table 4. Approval, certification, authorisation and reimbursement obstacles	50
Table 5. Interoperability drivers	57
Table 6. Interoperability obstacles	59
Table 7. Data protection and liability drivers	66
Table 8. Data protection and liability obstacles	66
Table 9. Professional qualifications drivers	70
Table 10. Professional qualifications obstacles	71
Table 11. Online sales of pharmaceutical products drivers	73
Table 12. Online sales of pharmaceutical products obstacles	73
Table 13. Regulatory development.....	75
Table 14. DiGA.....	78
Table 15. mHealth Belgium.....	78
Table 16. ANS eHealth Label	79
Table 17. HAS mHealth	79
Table 18. MAST CIMT	79
Table 19. Main areas of healthcare	90
Table 20. Rules involving a quality benchmark or criteria for AI-based systems in healthcare	98
Table 21. Common metrics used in evaluation of AI algorithms	99
Table 22. Hierarchical model of efficacy to assess the contribution of AI systems.....	101
Table 23. Rules adopted for the organisation and provision of healthcare when AI is involved	105
Table 24. EU regulations by type of issue addressed	108
Table 25. Regulatory framework for AI medical devices in the USA, Europe and Canada.....	117
Table 26 Rules on the conditions under which AI-based products are approved	120
Table 27. Rules on evaluation of AI health applications.....	121
Table 28. Rules on medical data gathering, organisation and use of medical data for developing AI in healthcare.....	128
Table 29. Rules on the access to algorithms used in healthcare	129
Table 30. Rules on the assessment of self-learning algorithms used in healthcare.....	130
Table 31. The main points of discussion relating to the application of PLD to AI.....	136
Table 32. Liability rules that were adopted for AI products and services in healthcare	137
Table 33. Framework for analysing characteristics that impact the value of a data set.....	147
Table 34. Realisation of the economic benefits resulting from the creation of an NHS longitudinal patient-level data set	151
Table 35. Summary of economic value to the UK NHS benefit to patients	152
Table 36. Estimated market value of health data per country	153
Table 37. Estimated total savings for Member States health services and benefits per patient per annum	155
Table 38. Estimated fixed cost of data permit authorities	158
Table 39. Estimated variable costs for data permit authority	160
Table 40. Government-funded platforms in which researchers can access health data for research purposes	180

Table 41. Examples of EU health infrastructures	181
Table 42. Examples of different legislative requirements for the EHRs in Member States	186
Table 43. Legislation or rules that facilitate data from the EHRs to be used/controlled by patients	187
Table 44. Legal bases for primary use of health data (normal healthcare provision)	188
Table 45. Legal bases for processing data for secondary purposes	192
Table 46. Sectoral legislation or authoritative guidance by Member States in the context of health research	193
Table 47. CEF Financing	204
Table 48. eHealth services availability across EU Member States	209
Table 49. Mobile contact tracing apps in EU Member States	211
Table 50. Rules to provide digital access to a copy of the medical record/s for patients affiliated to your healthcare system seeking cross-border healthcare in another Member States	216
Table 51. Rules to provide digital access to a copy of the medical record/s of received treatment/s for patients affiliated to a different healthcare system that used cross-border healthcare in your Member States	217
Table 52. Financing of eHealth Network Joint Actions	228
Table 53. Relevant EU projects	229
Table 54. Number of meetings carried out by the eHN during 2020 and 2021	230
Table 55. Overview costs and benefits	232
Table 56. Digital health products and services initial research questions	279
Table 57. Artificial intelligence in healthcare initial research questions	281
Table 58. Governing the use of health data initial research questions	284
Table 59. Evaluation of Article 14 of Directive 2011/24/EU initial research questions	284
Table 60. Digital health products and services search strings	287
Table 61. Artificial intelligence in healthcare search strings	288
Table 62. Governing the use of health data search strings	289
Table 63. Evaluation of Article 14 of Directive 2011/24/EU search strings	291
Table 64. Estimated economic value of heath data - EHR adoption	308
Table 65. Estimated economic value of heath data - Health Information Exchange (HIE) adoption	310
Table 66. Estimated economic value of heath data - Telehealth adoption	312
Table 67. Estimated economic value of heath data - Personal Health Record (PHR) adoption	314
Table 68. Estimated cost of cybersecurity breaches	317
Table 69. Next MFF instruments	325
Table 70. Mapping MWP 2012-2014 (eHGI JA)	327
Table 71. Mapping MWP 2015-2018 (JAseHn)	328
Table 72. Mapping MWP 2018-2021 (EHAAction)	330
Table 73. Common Semantic Strategy (CSS)	335

List of Figures

Figure 1. Overview methodology and reporting	21
Figure 2. Systematic map of research type and study focus	89
Figure 3. Main areas AI in health	91
Figure 4. AI systems typology	93
Figure 5. AI system phases in health	97
Figure 6. EHR sharing between health care professionals per Member State.....	165
Figure 7. Intervention logic framework	200
Figure 8. Financing of the eHealth Network during the eHGI JA (2012-2014)	203
Figure 9. JASeHN overall positioning	206
Figure 10. MyHealth@EU usage: number of ePrescription and Patient summaries exchanged	210
Figure 11. Member States readiness to implement the EU Digital COVID certificate Gateway	213
Figure 12. Total number of forms/claims received/issued by the Member States of affiliation	214
Figure 13. Total amount paid by the Member States of affiliation (in €)	214
Figure 14. Total number of claims received by the Member States of affiliation	215
Figure 15. Total amount of debits owed by the Member States of affiliation	215
Figure 16. Self-assessed results of Article 14 (a)	218
Figure 17. To what extent do you agree that the eHealth Network support contributes to a more cost-efficient development of cross-border digital health resources	233
Figure 18. AI system in health: problem, causes, gaps and proposed actions	249
Figure 19. Digital health products and services PRISMA diagram	288
Figure 20. Artificial intelligence in healthcare PRISMA diagram	289
Figure 21. Governing the use of health data PRISMA diagram	290
Figure 22. Evaluation of Article 14 of Directive 2011/24/EU PRISMA diagram	292

List of Boxes

Box 1. Article 14 of the Directive 2011/24/EU	20
Box 2. Scope	21
Box 3. Examples of European cross-border telemedicine projects	35
Box 4. The European University Hospital Alliance (EUHA)	36
Box 5. EUnethTA, a cooperation on eHealth technology assessment towards common schemes	37
Box 6. «CE» marking for medical devices	39
Box 7. Report of the Working Group on mHealth Assessment Guidelines (2017)	41
Box 8. Quality criteria: standards ISO/CEN 82304-2	42
Box 9. mHealth Hub framework and use cases	43
Box 10. Case studies – Bringing eHealth innovations into the market.....	46
Box 11. German Digital Healthcare Act.....	48
Box 12. Patient Summary implementation within Member states	52
Box 13. Article 14 of the Directive 2011/24/EU	57
Box 14. EHR authentication	60
Box 15. An example in Pomerania: the Telepom project	61
Box 16. International Medical Informatics Association Code of Ethics	63
Box 17. Privacy frameworks in North America	64

Box 18. National initiatives for eHealth skills and qualifications of healthcare professionals ...	69
Box 19. Example of the Aachen – Maastricht university hospitals collaboration.....	70
Box 20. Examples of legislative framework for the telemedicine in MS.....	76
Box 21. Article 17 of MDR	81
Box 22. Article 56 of TFEU	82
Box 23. Article 5(2) of the Directive 2005/36	82
Box 24. AI systems in health proposed definition.....	91
Box 25. Implementation of AI systems	103
Box 26. Australia's Therapeutic Goods Regulation.....	116
Box 27. Definitions of software as a device, by Section 3060 of the 21st Century Cures Act 2016	116
Box 28. FDA levels of clearance.....	118
Box 29. GDPR Art. 22. Automated individual decision-making, including profiling	122
Box 30. AI systems training process	123
Box 31. European Convention on Human Right Art 7 and 8.....	123
Box 32. GDPR Art 5. Principles relating to processing of personal data8	124
Box 33. GDPR Art 6 and 9	125
Box 34. GDPR Art. 22, 13 and 14	125
Box 35. Article 35 - Data protection impact assessment	126
Box 36. GDPR Art. 15 Right of access by the data subject	127
Box 37. Data Governance Act. Subject matter and scope (Art. 1)	142
Box 38. AIA Subject matter (Art. 1).....	144
Box 39. Significance of estimating total market value of health data	150
Box 40 Examples of fees for Findata data permits and requests	157
Box 41. Article 20 Right to Data Portability	164
Box 42. Darwin initiative	182
Box 43. Chapter 5 Transfers of personal data to third countries or international organisations	184
Box 44. National eHealth portal in Denmark.....	185
Box 45. Examples of variation across countries caused by the application of stricter rules at national level: France and the Netherlands	188
Box 46. Examples of specific legislation that obliges healthcare providers to provide patient data to public health authorities*.....	194
Box 47. Example of legislation on providing health data to insurers	195
Box 48. Specific objectives of the eHealth Network	197
Box 49. Operational objectives of the eHealth Network	198
Box 50. Intervention logic framework: Needs.....	199
Box 51. Main activities carried out	204
Box 52. Main outputs delivered	208
Box 53. Expected impacts.....	213
Box 54. Other EU policies and relevant EU documents.....	219
Box 55. Other relevant EU projects	220

Abstract

Health and healthcare services and products are rapidly changing due to new technologies, which can offer relevant solutions for healthcare services and products provided cross-border. This study investigates cross-border provision of digital health services and goods (eHealth), Artificial Intelligence and the use of health data. For each of the above-mentioned areas of the study the Consortium mapped and analysed the situation to provide the current picture of the topics of the study. To address the objectives of this study the team used a mixed methods approach, where different methods, instruments and sources have been triangulated. The detailed analysis allows for the identification of the key barriers at EU and national level, pointing the causes and consequences for stakeholders, as well as the potential evolution without EU intervention. The achievement of these specific objectives enabled a preliminary list of targeted areas for EU interventions. The study also evaluates the Cross-border Healthcare Directive (Directive 2011/24/EU), and more precisely Article 14 and related articles, which foresees the cooperation and exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by Member States.

Executive Summary

Healthcare services and products are evolving, and technological changes are driving this disruption. If used appropriately, innovative pathways supporting the transformation of healthcare systems have the potential of improving citizens' health outcomes, including healthcare provision across the Member States. As established by the Directive 2011/24/EU on patients' rights in cross-border healthcare¹, EU citizens have the right to access healthcare in any EU country and to be reimbursed for care abroad by their home country. Directive 2011/24/EU looks to facilitate access to those cross-border products and services by addressing issues related to healthcare costs, prescriptions and delivery of medications and medical devices. While more and more patients now can access digital services to manage their health, the level of adoption of such technologies varies across the EU Member States and remains limited in the context of cross-border provision of healthcare. The ability of healthcare providers and patients to communicate effectively in a cross-border healthcare setting remains one of the main obstacles to overcome for the Member States. The importance of investigating technological changes in the context of cross-border health has been further emphasised by the COVID-19 pandemic, which has threatened the right of free movement of people across the Member States².

This study provides the evidence needed by the European Commission to enable informed policymaking in the areas of:

- Digital health products and services (see chapter 2),
- Artificial Intelligence in health (see chapter 3),
- Governing the use of health data (see chapter 4),
- Evaluation of Article 14 of the Directive 2011/24/EU (see chapter 5).

Regarding digital health products and services, the study displays the current state of digital health regulatory and legal situation among the Member States as well as identifies several potential policy actions in the following areas: approval, certification, authorization, and reimbursement rules; data interoperability; privacy and liability rules; professional qualifications; online sales of pharmaceutical products.

The study also provides a comprehensive mapping and analysis of the current regulatory and legal situation on the adoption and use of Artificial Intelligence in healthcare across the EU and its Member States. The analysis identifies key factors hampering or enabling the adoption and use of Artificial Intelligence in the healthcare sector (including liability issues) with a particular focus on the cross-border aspect and the functioning of the single market.

In the area of governing the use of health data, the study focuses on the costs and benefits of primary use of data and exchange of health data for healthcare, as well as the further processing of health data for research, policy making and regulatory purposes (so called 'secondary use').

Finally, as part of the evaluation of Article 14 of the Directive 2011/24/EU, the study examines the effectiveness, efficiency, coherence, relevance, and EU added value of Article 14 of the Directive 2011/24/EU and other related articles.

To address the objectives of this study the team used a mixed methods approach, where different methods, instruments and sources have been triangulated (see section 1.3). Evidence

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0024>

² Article 3(2) of the Treaty on European Union (TEU); Article 21 of the Treaty on the Functioning of the European Union (TFEU); Titles IV and V of the TFEU; Article 45 of the Charter of Fundamental Rights of the European Union.

was gathered by triangulating primary and secondary sources. Secondary sources were collected by an initial scoping review followed by an additional desk research. Overall, 637 documents have been gathered and analysed for this study. The documents included academic literature as well as relevant studies, reports, research, legal documents. The initial findings were complemented by primary sources collected via stakeholders' consultation. The consultation included a total of 28 interviews, 9 focus groups and 2 online surveys. The consultation covered national bodies (Ministries of Health, eHealth agencies, National Medicines Agencies, institutions identified through the scoping review, etc.), European and international organisations (European Medicines Agency, Patients Organisations, Representatives of the MedTech Industry, Representatives of Healthcare Professionals, etc.) as well as private stakeholders (digital companies, medical devices companies, etc.).

The study finds several conclusions and recommendations (see chapter 6). With regards to digital health products and services, five needs have been identified, namely:

- Establish labelling/certification/authorisation guidance for digital health services and products.
- Define the scope of telehealth/mHealth products and services to be reimbursed.
- Facilitate the use of digital products/services and the access to patients' data.
- Ensure transparency of digital health services and products provided cross-borders.
- Ensure an appropriate liability framing for digital health.

For each need, different policy options have been provided.

With regards to AI systems in health, there is a slow and limited uptake of digital health products and services which integrate AI. The study identified several interrelated gaps that justify the slow uptake and that can be grouped in three main areas from a regulatory and governance point of view:

- Absence of a harmonised regulatory framework that addresses the specificities of AI systems in health.
- Lack of appropriate enabling environment for the flourishing of AI.
- Lack of trust and transparency.

The current proposed EU initiatives, Artificial Intelligence Act and the Data Governance Act (together with the forthcoming European Health Data Space), are establishing the ground to address most of the identified gaps. The study also provides additional recommendations to address the remaining needs and gaps.

This study finds that the main challenge and regulatory gaps for the exchange of health data for healthcare provision (primary purposes) is to ensure data security and effective compliance. In terms of challenges and regulatory barriers for the access of health data for research, innovation, policy making and regulatory decision (secondary purposes), the study finds that the current situation of fragmentation, differences in and barriers to access health data in the cross-border context, including by patients, researchers and policy-makers, as well as limited interoperability, shows that action by Member States alone is not sufficient and that it requires a common framework at EU level. The creation of a European Health Data Space (EHDS), supported by the THEDAS Joint Action goes into this direction. The study also provides additional policy options for both primary and secondary use of health data (see section 6.3). The evaluation of Article 14 of the Directive 2011/24/EU finds that, the effectiveness of the eHealth Network action has been very limited and concentrated in enhancing the use of health data for primary purpose in

the context of cross-border healthcare such as the development of the MyHealth@EU platform. The platform is currently able to run core primary use of data services (ePrescriptions and Patient Summary). Nevertheless, the low pick-up rate highlights a certain lack of coherence with national health policies and priorities. Furthermore, the provisions of Article 14 also include the objective of supporting the innovative use of health data for secondary purposes, an area where little to no activities have been carried out until the establishment of the THEDAS Joint Action. While the eHealth network proved to be effective and efficient in times of political convergence following the COVID 19 pandemic outbreak, previous initiatives presented some issues in terms of efficiency, especially when the initiative was not legally supported by a regulation. Most of the initial needs supporting the establishment of the eHealth Network are still relevant today. The digitalisation of healthcare has actually increased the need for greater interoperability and data flow also in the context of telehealth and mHealth. Overall, while the pool of people potentially benefitting from cross-border healthcare is high, the patients taking advantage of this possibility is currently low although increasing. Based on the results provided in the study, several recommendations have been developed with regards to article 14 of the Directive 2011/24/EU (see section 6.4).

1. Background and methodology

1.1 Context of the study

The rapid uptake of new technologies and the growing digital health market have the potential to offer relevant solutions for healthcare services and products provided cross-border. Indeed, digital technologies provide innovative pathways supporting the transformation of healthcare systems and improving citizens' health outcomes. EU citizens have the right to access healthcare in any EU country and to be reimbursed by their home country when receiving care abroad. The cross-border healthcare Directive (2011) looks to facilitate access to all healthcare services across Member States and sets out the conditions under which a patient may travel to another EU country to receive medical care and reimbursement. It covers healthcare costs, prescriptions and delivery of medications and medical devices. However, the ability of healthcare providers and patients to communicate effectively in a cross-border healthcare setting remains one of the main obstacles to overcome for Member States. The COVID-19 pandemic has emphasised the importance of providing such services and ensuring timely access to health data.

Based on the Directive, Member States collaborate through a voluntary network (the 'eHealth Network') which connects national authorities responsible for eHealth. However, the arrangements and tools given to Member States only provide partial answers to current challenges. Despite the surge in the access and use of digital services by patients to manage their own health, the level of adoption varies across the Member States. The lack of relevant national legislation and the flaws of applicable EU legislation implementation could pose a threat to the cross-border provision and the safety of digital health services, and therefore severely impact free movement between Member States.

The European Health Data Space (EHDS) has become a priority to make digital health thrive. It aims at improving health outcomes by promoting access to health data for innovation and research of new preventive strategies and diagnosis and treatment of diseases, while ensuring that citizens have control over their own personal data.

This Final Report is structured around 6 chapters. Chapter 1 presents the objectives and scope of the different areas covered in this study together with the methodological approach and the limitations. Chapter 2 elaborates on the findings for digital health services and products, including definitions, different application areas, the main components that help cross-border digital health thrive, and current regulatory practices and gaps, different approaches between Member States and EU laws, and legislative inhibitors that can be found in the industry. Chapter 3 provides up to-date mapping on the current regulatory and legal situation of Member States for AI in the healthcare sector, including liability issues, as well as key inhibitors and drivers for the adoption and use of AI in the healthcare sector. Chapter 4 describes the current Member State regulations as well as the drivers and inhibitors for the use and access of healthcare data for healthcare provision, research, policymaking, and regulation. Chapter 5 examines the effectiveness, efficiency, coherence, relevance, and EU added value of Article 14 of the Directive 2011/24/EU and other related articles as well as its impact on cross-border healthcare/patient mobility, the provision of digital health services and products, and national healthcare systems. Finally, Chapter 6 presents policy recommendations and conclusions for each one of the topics detailed in the previous chapters.

1.2 Objectives and scope

The main objective of the "Study on cross-border digital healthcare in the EU with particular focus on potential regulatory gaps and barriers to the cross-border provision of digital health services and products" is to provide the evidence base needed by the European Commission to

enable informed policy making in the area of cross-border provision of digital health services and goods. This will help with the accessibility, availability, and affordability of high-quality healthcare around the structuration of the EHDS, as well as foster a genuine single market for digital health products and services.

1.2.1 Digital health products and services

eHealth comprises the provision of healthcare product and services using ICT (Information and Communication Technology). It includes the use of digital products, services or processes and is combined with an organisational change in healthcare systems, to improve public health, as well as accessibility, efficiency and productivity in healthcare delivery. “eHealth (including mHealth and Telehealth) services and products” topic focuses on the following aspects: (1) Approval, certification, authorization and reimbursement rules; (2) Interoperability; (3) Privacy and liability rules; (4) Professional qualifications; (5) Online sales of pharmaceutical products. As a result, the purpose is to display the current-state of digital health regulatory and legal situation among the Member States as well as to identify several potential policy actions that support their cross-border use and foster the European market

1.2.2 Artificial intelligence in health

The development of artificial intelligence (AI) in health is currently experiencing a very strong acceleration with the broad multiplication of applications, particularly in the field of image recognition in radiology, ophthalmology or dermatology. Algorithmic medicine has already become a reality and will become increasingly important in the years to come. Despite the potential benefits of AI in the field of health, there are a number of elements which should be taken into account, and which should be integrated for these innovations to be established in society (Aulas et al, 2019).

AI technology is commonly understood as intelligence displayed by machines, the ability and development of machines to perform tasks that normally require human intelligence, or some such variation (Chung & Zink, 2017). In the 1950s the concept of Artificial Intelligence (AI) was created and, in the following years, different techniques and types of AI have emerged. AI encompasses machine learning, the scientific discipline that uses computer algorithms to learn from data, to help identify patterns in data, and make predictions (Collins & Moon, 2019). AI is being used to replace humans at an increasing number of junctures in the decision-making process in numerous in numerous industries. This, however, also means that there are fewer and fewer opportunities for humans to inject their judgment (Chung & Zink, 2018).

The health sector stands to be one of the major beneficiaries from the application of AI in their daily routines, both in terms of logistics and in terms of healthcare management. These data-driven technologies form the basis of the digital healthcare revolution provide potentially important opportunities to deliver improvements in individual care and to advance innovation in medical research. Among the most compelling applications of AI is the use of predictive algorithms in precision medicine (Sullivan & Schweikart, 2019).

There are still many challenges to obtain full benefits of AI in healthcare, such as the access to data, regulations specifically set up for AI in healthcare, technical issues associated with the complexity of AI algorithms, and unresolved legal and ethical questions. The EU pays close attention to these challenges in its strive to develop a coherent strategy and appropriate policy frameworks for AI. The Proposal for a Regulation on European data governance (Data Governance Act - DGA)³ would address the availability of public sector data for re-use in

³ COM(2020) 767 final

situations where such data is subject to rights of others; data sharing among businesses, against remuneration in any form; ‘personal data-sharing intermediary’, designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR) and data use on altruistic grounds. The DGA specifically mentions the creation of the European Health Data Space.

In addition, with the proposal for a regulation on Artificial Intelligence (also referred to the Artificial Intelligence Act⁴), the EC is proposing the first ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally. Thus, health systems should be prepared to receive these new applications so the benefits of AI can be received and understood by all the related stakeholders: patients, healthcare professionals, and society.

More specifically in the Artificial Intelligence in the healthcare sector, the objectives are:

- To provide an up-to-date and comprehensive mapping and detailed analysis of the current regulatory and legal situation in the EU and its Member States with regard to the adoption and use of Artificial Intelligence in the healthcare sector (including liability issues).
- To identify the key factors hampering or enabling the adoption and use of Artificial Intelligence in the healthcare sector (including liability issues) with a particular focus on the cross-border aspect and the functioning of the single market.
- To provide a preliminary list of conclusions and recommendations within the current proposed legislative initiatives.

These objectives were complemented with guiding research questions (see Annex 8.1).

1.2.3 Governing the use of health data

EU citizens have the right to access healthcare in any EU country and to be reimbursed for care abroad from their home country. Directive 2011/24/EU on Cross-border Healthcare sets out the conditions under which a patient may receive medical care in another EU country and seek reimbursement for such care in complementarity to other EU rules on reimbursement of social claims such as the Electronic Exchange of Social Security Information (EESI). It covers healthcare costs, as well as the prescription and delivery of medications and medical devices. The Directive facilitates access to healthcare services across Member States, in particular information on available healthcare in other European countries, alternative healthcare options and/or specialized treatment abroad.

In this context, the access to health data and the exchange and usage for primary and secondary purposes is key to facilitating the cooperation and exchange of information both nationally and cross-border in the EU. The objective of the “Study on cross-border digital healthcare in the EU with particular focus on potential regulatory gaps and barriers to the cross-border provision of digital health services and products” and especially of “Governing the use of Health Data” (Lot 3) is to examine the following aspects:

- Primary use of data and exchange of health data for healthcare and the costs and benefits
- Further processing of health data for research, policy making and regulatory purposes and the costs and benefits (so called ‘secondary use’).

⁴ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. COM(2021) 206 final.

1.2.4 Evaluation of Article 14 of Directive 2011/24/EU

The objective of this topic was to examine the effectiveness, efficiency, coherence, relevance and EU added value of Article 14 of the Directive 2011/24/EU and other related articles and to describe the impact of Article 14 of the Directive 2011/24/EU on cross-border healthcare/patient mobility, the provision of digital health services and products, and national healthcare systems.

In this study, we analysed the current situation for different eHealth stakeholders across the EU and how the current regulatory and legal situation in the EU and its Member States is affected by the application of the Directive, as well as an overall elaboration of how eHealth has been deployed and facilitated since the adoption of the Directive, considering the voluntary base of the eHealth Network (eHN).

According to the better regulation guidelines⁵, evaluations allow the Commission to constantly collect and analyse information about the performance of the Union's policies. The aim is to ensure that objectives continue to be met without imposing unnecessary costs on society.

More concretely, an evaluation is an evidence-based judgement of the extent to which an existing intervention is:

- Effective;
- Efficient;
- Relevant given the current needs;
- Coherent both internally and with other EU interventions; and
- Has achieved EU added value.

The rapid uptake of new technologies and digital solutions have the potential to offer relevant evolving solutions for health and healthcare services and products, providing the possibility to overcome the current main challenges of the different national healthcare systems. The ability of healthcare providers and patients to communicate effectively with each other is one of these challenges and requires the facilitation of the provision of digital health services in a cross-border setting. EU citizens have indeed the right to access healthcare in any EU country, as well as to be reimbursed for care abroad by their home country, within the limits provided for by the applicable EU legislation. The Cross-border Healthcare Directive sets out the conditions under a patient may access healthcare to another EU country to receive medical care and reimbursement. It covers healthcare costs, as well as the prescription and delivery of medications and medical devices. The Directive intends to facilitate the access to safe and high-quality healthcare services across the Member States).

The Cross-border Healthcare Directive (2011/24/EU) provides a specific framework for access to healthcare in another EU Member State and for its reimbursement. In doing so, it clarifies issues surrounding the responsibility of the Member States for ensuring quality and safety standards, provision of information, redress and systems of liability insurance, as well as privacy protection. In addition, it endeavours to foster European cooperation on healthcare in specific areas. Article 14 of the Directive 2011/24/EU, concerning eHealth, assigned the Union to support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States (the 'eHealth Network'). The same article sets the objectives of the eHealth Network and empowers the Commission to adopt the necessary implementing measures for the

⁵ https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en#:~:text=The%20better%20regulation%20guidelines%20set,of%20the%20law%2Dmaking%20cycle.

Network's establishment, management and transparent functioning. As more and more patients now can access digital services to manage their health, the level of adoption of such technologies varies across the Member States, with different approaches in the field of these digital cross-border health services. As a consequence, different rules have been implemented by the Member States, and either a lack of relevant national legislation or shortcomings in the "*cooperation and the exchange of information*" could pose a threat to the cross-border provision and safety of digital health services, with severe impacts on the patients/citizens free movement between Member States.

Box 1. Article 14 of the Directive 2011/24/EU

1. The Union shall support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States.
2. The objectives of the eHealth network shall be to:
 - (a) work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare;
 - (b) draw up guidelines on:
 - i. a non-exhaustive list of data that are to be included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across-borders; and
 - ii. effective methods for enabling the use of medical information for public health and research;
 - (c) support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.

The objectives referred to in points (b) and (c) shall be pursued in due observance of the principles of data protection as set out, in particular, in Directives 95/46/EC and 2002/58/EC.

3. The Commission shall, in accordance with the regulatory procedure referred to in Article 16(2), adopt the necessary measures for the establishment, management and transparent functioning of this network.

Source: Directive 2011/24/EU

The scope of this report is not strictly limited to article 14 of the Directive 2011/24/EU, but it also considered related legal provisions where relevant for the assessment of the EU cooperation on eHealth, including work of the eHealth Network. An illustrative list of such provisions is provided in Box 2. While Article 14 is the main focus of this study, we have also addressed elements related to interoperability of ePrescriptions, patients access to a written or electronic medical record after receiving treatment and telemedicine reimbursement. Other provisions of the Directive 2011/24/EU will be evaluated by the study SANTE/2021/B2/011 and therefore fall outside the scope of this study.

Box 2. Scope

Article 11.2 (b)

In order to facilitate implementation of paragraph 1 (Recognition of prescriptions issued in another Member State), the Commission shall adopt:

- (b) guidelines supporting the Member States in developing the interoperability of ePrescriptions

Article 4.2 (f)

The Member State of treatment shall ensure that:

- (f) in order to ensure continuity of care, patients who have received treatment are entitled to a written or electronic medical record of such treatment, and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC.

Article 5 (d)

The Member State of affiliation shall ensure that:

- (d) patients who seek to receive or do receive cross-border healthcare have remote access to or have at least a copy of their medical records, in conformity with, and subject to, national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC.

Article 7.7

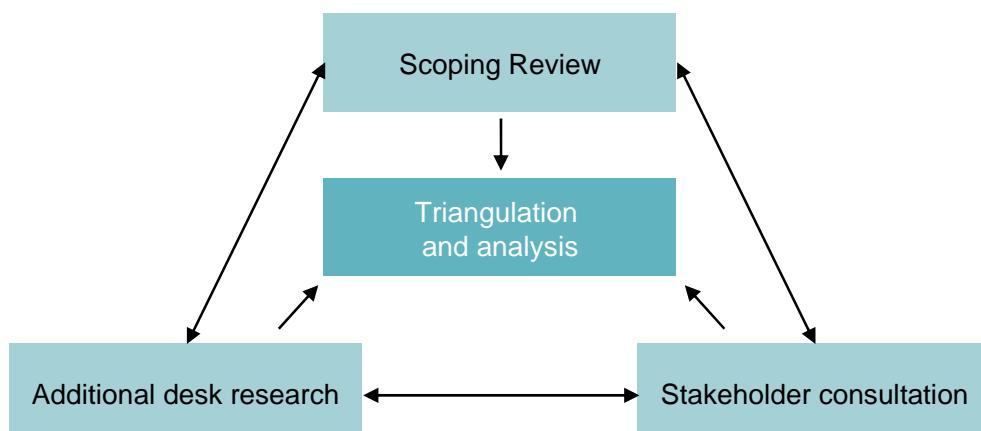
The Member State of affiliation may impose on an insured person seeking reimbursement of the costs of cross-border healthcare, including healthcare received through means of telemedicine, the same conditions, criteria of eligibility and regulatory and administrative formalities, whether set at a local, regional or national level, as it would impose if this healthcare were provided in its territory.

Source: Directive 2011/24/EU

1.3 Methodological approach

The study was conducted using a **mixed-methods approach** where we triangulated different methods/instruments and different sources (primary and secondary). A mixed-method approach enables to shed light on complex policy issues where the results of experiments or survey alone would not be sufficient to draw some policy implications and recommendations. The figure below sketches the methodological approach. An initial scoping review was followed by additional desk research and complemented by a stakeholder consultation.

Figure 1. Overview methodology and reporting



Source: Author's elaboration

1.3.1 Scoping review and desk research

An extensive documentary review was conducted between September and October 2020 to gain the most updated and comprehensive literature to answer the research questions guiding this study. The review process was designed as a roadmap detailing the objectives, the search procedure and the inclusion criteria. To collect thorough knowledge, both the scoping review and the desk research were conducted following systematic principles, which are described under this section.

The research team used the previously tested search strings on two databases, namely ISI Web of Science and PubMed. The search strings were tailored to inform the research questions guiding the study. A detailed summary of the search strings and number of hits is summarised in Annex 8.2.

Following the proposed exclusion criteria, we discarded the following: (1) publications not answering one or more of the research questions outlined, (2) works published before the cut-off date 2015, (3) publications that do not touch upon the geographical scope of interest, with the scope of interest comprising of EU Member States and, in some cases, best practices and regulations of other countries such as the United States and Canada. Given the broad scope of the review as concerns the study type and design, no limits or restrictions were set on the type of study design. Additionally, a targeted desk research exercise was conducted in order to ensure that the study includes all relevant studies, reports, research, legal documents and materials issued or endorsed by all the Member States authorities, EU institutions, European or national stakeholders' associations or individual stakeholders. The full summary of desk research identified is shown in Table 1.

As for the research of the legal documentation and case law, the Consortium has mapped national legal acts and provisions related to the transposition of Directive 2011/24/EU, all relevant case law that has been filed at the national level, national eHealth strategies, as well as national law and Union provisions on the protection of personal data (in particular Regulation 2016/679/EU) that could prove relevant to identify barriers on cross-border provision of healthcare. In addition, the Consortium retrieved all the available information from the eHealth Network since 2011 on needs, objectives, input, activities and outputs and results. The documentation that was not available online was requested to DG SANTE. This exercise resulted in a pool of 83 documents that were screened and summarised in the present report.

1.3.2 Stakeholders' consultations

Consultation strategy

The work conducted for the consultation was firstly intended to identify the different eHealth stakeholders and the way they are affected by the 2011/24 EU Directive. This work led to a stakeholders mapping, identifying 223 stakeholders, detailing their Member State of influence, their category, their influence level, and their relation to the Directive. The mapping covered national bodies (Ministries of Health, eHealth agencies, National Medicines Agencies, institutions identified through the scoping review, etc.), European and international organisations (European Medicines Agency, Patients Organisations, Representatives of the MedTech Industry, Representatives of Healthcare Professionals, etc.) as well as private stakeholders (digital companies, medical devices companies, etc.).

Since the consultation phase also aimed to dive into the targeted gaps, the data collection findings and the gap analysis fed into this work. Using both the stakeholders mapping and the previous analysis, around 15 specific stakeholders were targeted. The objective was to have a diverse range of stakeholders in the types of institutions they work in and the roles they have

within those institutions. Their roles in their organizations made them the most fitting to provide answers to as many research and ad-hoc questions the research team had.

The consultation phase had three different methods designed to reach stakeholders efficiently: (1) in-depth interviews, (2) focus groups and (3) online surveys. The summary of the consultation phase and desk research is shown in Table 1. The guidelines supported the interviews and focus groups and highlighted what issues and questions would be tackled by the different stakeholders. The minutes of each interview and focus group carried out were sent both to the participants for validation and to the DG SANTE for information. All the main inputs collected from the consultation, along with the associated outcomes, were included in the overview of the current state regarding eHealth services and products, the analysis of drivers, obstacles, costs and benefits per area, as well as the identification of regulatory gaps.

Table 1. Summary table of consultation phase and desk research

Outcome metrics	Desk research retrieved	Interviews	Focus Groups	Online survey
Digital health products and services	115	7	2	1
Artificial intelligence and health	143	6	2	1
Governing use of health data	176	9	3	1
Evaluation of Article 14 of Directive 2011/24/EU	203	6	2	2
Total	637	28	9	2*

*One online survey covering all topics was pre-filled by the Consortium and sent to the eHealth Network members. For the Evaluation of Article 14 of Directive 2011/24/EU a further complementary survey was developed and submitted to the focus group participants.

Source: Author's elaboration

In-depth interviews

The different fieldwork activities were then used to complement the primary sources collected and the information gap identified during the initial part of the study. In-depth interviews took the form of a conversation and most of the questions asked lead us to follow-ups to elicit further details, tapping into the knowledge, experiences and vision of the expert interviewees on the basis of their expertise / experience related to the issue at stake. This means that this interview protocol left room for elaboration or additional questions to maintain flexibility within interviews. This semi-structured approach thereby ensured a similar set of questions being asked of all stakeholders but allowing targeted questions for particular stakeholders that share a particular interest in the topic. Potential interviewees were contacted by telephone /email, informed about the aims and objectives of the study and the funding agency (European Commission, DG SANTE), and invited to take part in the study. Then, the interested stakeholders have been provided with a concise description of the study, and information regarding the details of the study and an accreditation letter from DG SANTE, consent to take part in the interview, attribution of information, confidentiality and audio-recording of the interview consent. In total, 28 expert interviews across all lots were conducted during January, February, and March 2021. To see a summary of all interviews conducted, see Annex 8.3.

Digital health products and services. A total of 7 in-depth interviews were conducted with stakeholders from various backgrounds chosen according to the stakeholders mapping in order to use a diverse pool with different perspectives. These interviews were intended to collect

hands-on knowledge and qualitative insights on the field related to the provision of cross-border digital healthcare, as well as potential regulatory gaps and related obstacles.

Artificial intelligence in health. Seven expert interviews were carried out for each of the six different areas were discussed: 1) behavioural impact interview: perspective from medical professional background, 2) behavioural impact interview: perspective from patient associations, 3) behavioural impact interview: perspective from professionals, 4) future regulation of AI in the healthcare sector , 5) eHealth assessment and labelling, eHealth services / products adoption, AI services in healthcare, Health data sharing / access and 6) industry perspective of AI use in the healthcare sector, respectively.

Governing the use of health data. As part of the stakeholders' consultations, 9 Expert interviews were carried out to gain in-depth understanding on the drivers and barriers of data sharing per stakeholder as well as national law and EU provisions on the protection of personal data.

Evaluation of Article 14 of Directive 2011/24/EU. 6 Expert interviews carried out to gain in-depth understanding on the application of Art. 14 and accompanying acts, as well as the effectiveness, efficiency and coherence of the activities carried out by the eHealth Network since its set up in 2012. The interviews targeted representatives of the industry and of patients, as well as co-coordinators of current and past Joint Actions supporting the eHealth Network and the European Health Data Space (THEDAS).

Focus groups / workshops

The complete list of summarised focus groups/workshops, including the areas covered and an overview of participants, is presented in Annex 8.3.2.

Digital health products and services. A total of two focus groups were conducted for this area with stakeholders from various backgrounds with an appropriate mix of fields of expertise. The first focus group concentrated on: the practical provision of digital health services at a cross-border level, privacy, and professional qualifications recognition. It involved healthcare professionals and digital health industry representatives (RSCN, Standing Committee of European Doctors, COCIR). The second focus group discussed the assessment of mobile health and the practical implementation of a quality label to support the uptake of digital health services and products. It involved eHealth experts on digital services assessment along with HTA representatives.

Artificial intelligence in health. A total of two workshops were conducted. The first workshop dealt with "US and legal perspective", where the experts discussed: overview of AI uses in healthcare, manufacturer's liability for three types of defects, causation, burden of proof on plaintiff, relationship between physicians and AI manufacturers for continuously learning AI, learned intermediaries, experts in the field and consumer advertising and unavoidable unsafe products. The second workshop focused on "AI Liability in health - practitioners' perspective" and addressed the following topics: liability questions arising from AI systems in healthcare; behavioural impacts of the use of AI systems, industry perspective and future regulation and cost-benefit considerations of AI systems in healthcare

Governing the use of health data. A total of three workshops were carried out during March and April 2021. The first workshop addressed costs and benefits of the use of health data for healthcare provision and the access of health data for research, policy-making, and regulatory purposes. The second workshop was organised with members of the Towards the European Health Data Space Joint Action project and addressed current EU-level structures for health data

sharing and national data governance models. Finally, the third interview for this topic was a small break-out session that went into more depth of the previously mentioned workshop topics.

Evaluation of Article 14 of Directive 2011/24/EU. Two workshops carried out during March 2021. While the first workshop was organised with the eHealth Network and focused more on the evaluation of the activities carried out, the second workshop was organised with a broad range of experts and focused mainly on future needs⁶.

Online surveys

One unique online survey was developed covering all the areas for the study. The aim was to strengthen the global overview on the existing legal frameworks in every European Member State. To facilitate both participation and data processing, the questionnaire relied firstly on "yes/no" questions related to the original research questions and focused on the national existing and/or future legislative frameworks on every assessed topic. The survey also included dedicated areas for additional comments and precise inputs from the respondents on each key topic.

This online survey was sent to the Consortium eHealth experts' networks from each Member State. The inputs collected from the responses helped to complete each Members State's country factsheet. They brought an additional perspective and legislative inputs on the regulatory and legal aspects in the area of eHealth services and products, both locally and in a cross-border context.

Evaluation of Article 14 Directive 2011/24/EU. One complementary survey submitted to all the eHealth Network members in April 2021 to complement the first workshop and gather additional information on the evaluation of the activities carried out by the eHealth Network. The objective was to gain a clear picture of the current situation of cross-border provision of digital healthcare across the EU and access to health data for secondary use. A total of 19 Member States and Norway provided complementary inputs.

To note, Chapter 5, the Evaluation of Article 14 of Directive 2011/24/EU, also includes findings from other areas of the study:, including different aspects of eHealth, telemedicine and mHealth, among which some are particularly relevant areas, such as approval, certification, authorization and reimbursement rules, interoperability, as well as privacy and liability rules; and primary use of data and exchange of health data for healthcare as well as the further processing of health data for research, policymaking and regulatory purposes.

Both questionnaires are presented in Annex 8.2.

1.3.3 Analysis and triangulation

Each article was summarised to highlight the most important outcomes to be included in the study. These summaries were used to build a narrative for the overview of the current state of cross-border health care.

The comparison between the first findings and the initial research questions led to a gap analysis addressing the main issues we came across and the answers which could already be found or not. The research team elaborated on the findings of the data collection and targeted the aspects that needed to be covered or complemented. The team, together with DG SANTE, used the outcomes from the gap analysis of all research areas to help with the stakeholder's consultation. According to these preliminary results and the insights identified on the potential impacts on the cross-border provision and free movement, a gap analysis table was built, providing a

⁶ A third relevant workshop on secondary use of data was carried out within the participation of the TEHDA members.

comprehensive overview of the gaps to be addressed during the consultation phase and some preliminary answers to identified issues.

A cross-analysis on all sections was conducted simultaneously on all study areas. For example, although the chapter “eHealth services and products” focuses on eHealth, telemedicine and mHealth, it is not self-sufficient and can benefit from the expertise of other chapters “Artificial Intelligence in healthcare sector”, “Use of health data” and “Evaluation of Article 14 of the Directive 2011/24/EU”. eHealth development among Member States relies on the development of appropriate and efficient data sharing infrastructure and reliable AI services. A common narrative was built to address in-depth interconnections between the sections of the study, especially on common topics such as liability and approval of digital health services and products, including AI-based tools and data infrastructures for health data storage.

1.4 Limitations of the study

This analysis is based on the best available evidence drawn from the triangulation a diverse and appropriate range of methods and sources. Where secondary sources were not available to answer the research questions guiding this study, primary data and evidence was collected. The intrinsic characteristics of scoping reviews often lead to broad, less defined searches that require multiple structured strategies focused on alternative sets of themes. A complementary desk research exercise was conducted to ensure the completeness and validity of the results obtained. The principal limitation that this type of methodology is an intrinsic limitation coming from literature that may not cover all the information available. The suggestions of policy options reflect the views and perception of the Consortium. This does not mean the European Commission endorses or recommends these policy options.

Another limitation was accurately quantifying costs and benefits of the access and exchange of health data by stakeholders. The nature of quantifying this process is complex due to the uniqueness per case and hard-to-measure realisation of outputs.

Limitations specific to the evaluation of Article 14 of Directive 2011/24/EU. By the end of 2020, only 7 Member States used the MyHealth@EU infrastructure to exchange Patients Summary and/or ePrescriptions (Croatia, Czechia, Estonia, Finland, Luxembourg, Malta, Portugal). Since the exchanges on the platform for the early adopters only started in 2019, the full potential of the platform has not been observed yet. Furthermore, the results suggest that most exchanges happen across neighbouring countries. Of the early adopters, only Finland and Estonia are neighbouring countries, limiting even more the exchanges on the platform. As 8 more Member States (Cyprus, France, Greece, Hungary, Netherlands, Poland, Spain, Sweden) are expected to join the platform in 2021 and all Member States by 2025, we can expect that over time there will be more information to assess the results and impacts in this area.

Furthermore, quantitative data on the costs of implementing the infrastructure were limited as the Member States that did implement the infrastructure were not able to quantify the costs in terms of man-days and budget allocated to it. Often, eHealth Network members did not keep appropriate accounting of the effort invested in carrying out eHealth Network activities and did not split this work from the one conducted for their national institutions. As a result, in the area of efficiency (A18), the information is mostly qualitative and resulting from expert’s opinions.

2. Digital health products and services

This section of the study, "eHealth (including mHealth and Telehealth) services and products", focuses on the following aspects: (1) Approval, certification, authorization and reimbursement rules; (2) Interoperability; (3) Privacy and liability rules; (4) Professional qualifications; (5) Online sales of pharmaceutical products. As a result, the purpose of this section is to display the current-state of digital health regulatory and legal situation among the Member States as well as to identify several potential policy actions that support their cross-border use and foster the European market.

2.1 Scoping the field

2.1.1 Definitions

eHealth

eHealth (Electronic Health) comprises the provision of healthcare products and services using ICT (Information and Communication Technology). It includes the use of digital products, services or processes and is combined with an organisational change in healthcare systems, in order to improve public health, as well as efficiency and productivity in healthcare delivery.

This definition is not legally accepted. However, the common characteristics between definitions could legally lead to a common European definition of these terms. It is to be noted that some definitions do have more in-depth definitions of concepts, but overall, there is a lot of overlap.

European Union. The European Union (EU)⁷ specifies that eHealth applies to the full range of professions in the health sector and has the potential to innovate and improve access to care, quality of care, and to increase overall efficiency of the health sector. According to the European Commission⁸, both eHealth and telemedicine are governed by freedom of movement of services, fully applicable to health care, and considered applicable to eHealth via the eCommerce Directive. Aligned with the general definition, the EAHP (European Association of Hospital Pharmacists) stated that "eHealth, or electronic health, refers to healthcare services provided with the support of ICT -such as computers, mobile phones and satellite communications- for health services and information".

North America (USA, Canada). The FDA (2016) uses the term "eHealth" to describe a broad array of digital information tools, ranging from electronic health records (EHRs), which facilitate the exchange of patient data between health care professionals, to computerized physician order entry mechanisms, e-prescribing, and clinical decision support tools, which provide information electronically to providers about protocols and standards for use in diagnosis and treatments.

Worldwide. Oh et al. (2005) analysed 51 unique published definitions and concluded that "the term eHealth encompasses a set of disparate concepts, including health, technology and commerce". The definitions include these concepts with varying degrees of emphasis but each one specifically refers to health and technology involved. Many note the varying stakeholders, the attitudes encompassed, the role of place and distance, and the real or potential benefits expected of eHealth. It is important to note that the technology is described as "a means to expand, to assist, or to enhance human activities, rather than as a substitute for them". The World Health Organization (WHO) has defined eHealth as "the cost-effective and secure use of information and communications technologies in support of health and health-related fields,

⁷ eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century

⁸ Commission of the European Communities. COM (2008)689 on telemedicine for the benefits of patients, healthcare systems and society.

including health-care services, health surveillance, health literature, health education, knowledge and research" (Catan et al., 2015). The variation in definitions reflects the various perspectives, settings and contexts in which eHealth is used. eHealth is considered an emerging field in the intersection of medical informatics, public health and business. It covers the interaction between patients and health-service providers, institution-to-institution transmission of data, and peer-to-peer communication between patients and/or health professionals. Since health can be understood as physical, mental and social well-being, eHealth revolves around using digital tools and sharing information digitally to achieve and maintain a good level of health, including wellness services. In a broader sense, the term can even characterize "not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology" (Eysenbach et.al, 2001 in BoogerdTessa et al., 2015).

Telemedicine/Telehealth

Telemedicine is the provision of healthcare services and medical information using innovative technologies, especially Information and Communication Technologies (ICT), in situations where the health professional and patient (or two health professionals) are not in the same location. It includes any remote interactions between patients and healthcare professionals, and between healthcare professionals themselves, whether synchronous or asynchronous.

A growing number of countries (including North American countries) consider that telehealth is a component of eHealth that encompasses a broader scope of technologies and healthcare providers than telemedicine, which refers specifically to clinical health services.

This definition is not legally accepted. However, the common characteristics between definitions could legally lead to a common European definition of these terms. It is to be noted that some definitions do have more in-depth definitions of concepts, but overall, there is a lot of overlap.

European Union. In 2019, the eHAction issued the latest definition of telehealth⁹ as "the delivery of healthcare services by Healthcare Professionals using ICT to provide clinical and non-clinical services – preventive, promotive and curative healthcare services, research and evaluation, health administration services". The terms "telehealth" and "telemedicine" have been used interchangeably, and according to Larsen et al. (2016), "telemedicine can also be used as an umbrella term for all the 'tele-' labels that are sometimes used rather indiscriminately to denote the use of information and technology to support healthcare services. However, strictly speaking, telehealth can be viewed as a higher level (parent) category covering many areas. Indeed, telehealth is in turn an expansion of the term telemedicine, which focuses more narrowly on the curative aspect¹⁰.

The definition provided by the European Commission¹¹ is adopted with slight adaptations in many European countries, where telemedicine is considered to improve prevention, diagnosis, treatment, monitoring, management of health and lifestyle. Although telemedicine is exclusively focused on healthcare, the EC stresses that telemedicine telecommunication systems are not devices (COM (2008)689). For Tsioumanis et al. (2016), it includes "the examinations, monitoring and treatment, as well as the educational sessions of patients and medical staff, processed by using systems, which allow the direct access to expert-members of qualified

⁹ http://ehaction.eu/wp-content/uploads/2021/01/eHAction_D4.1_Policy-Framework-People-Empowerment_Final.pdf

¹⁰ <https://www.eu-patient.eu/globalassets/projects/chainoftrust/epf-report-web.pdf>

¹¹ Commission of the European Communities. COM (2008)689 on telemedicine for the benefits of patients, healthcare systems and society.

personnel and to information about their patients, regardless the location of the patient and the relevant information". Telemedicine may be synchronous and/or asynchronous and may apply to any information and technology-based means of connecting healthcare actors and patients, such as video communication, e-mail, electronic monitoring equipment, and Internet portals¹².

The Consiglio Superiore della Sanita in Italy¹³ (2017) also defined what telemedicine is not, given that "the use of ICT tools for the processing of health information or the online sharing of data and/or health information are not in themselves telemedicine services". For example, the following elements are cited not to be included in the definition: information portals, social networks, forums, newsgroups, or electronic mail.

In France, telemedicine as defined in Article L. 6316-1 of the "Code de la Santé Publique"¹⁴ includes "medical acts performed at a distance by means of a device using information and communication technologies", namely:

- **Teleconsultation**, the purpose of which is to enable a medical professional to give a remote consultation to a patient (a health professional may be present with the patient and, if necessary, assist the medical professional during the teleconsultation);
- **Tele-expertise**, the purpose of which is to enable a medical professional to seek the opinion of one or more medical professionals at a distance because of their training or skills, on the basis of medical information related to the care of a patient;
- **Remote medical monitoring**, the purpose of which is to enable a medical professional to remotely interpret the data necessary for the medical monitoring of a patient and, when appropriate, to take decisions related to the care of that patient. The recording and transmission of data may be automated or carried out by the patient himself or by a health professional;
- **Remote medical assistance**, the purpose of which is to enable a medical professional to assist another health professional remotely during the performance of a procedure;
- **Medical response** which is provided within the framework of the medical regulation.

In Latvia Medical Treatment Law¹⁵, some regulatory definitions have also been introduced and define more simply telemedicine as the "provision of remote health care service, by using information and communication technologies", including "safe resending of medical data and information necessary for medical treatment in the form of text, sound, pictures or other". The Polish Telemedicine and eHealth Society considers telemedicine to cover the entire spectrum of medical services, including liability and licensing (see annex 8.4.1).

North America. The FDA stressed in 2016 that although the terms "telemedicine" and "telehealth" can be used to describe similar types of technologies, the term "telemedicine" has historically been used to refer specifically to bilateral, interactive health communications with clinicians on both "ends" of the exchange. The term "telehealth" incorporates not only technologies that fall under "telemedicine," but also direct electronic patient-to-provider interactions as well as the use of medical devices to collect and transmit health information. According to the American Telemedicine Association, the term "telemedicine" means "the use of medical information exchanged from one site to another via electronic communications to improve a patient's clinical health status, including applications and services using two-way

¹² https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf

¹³ http://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf

¹⁴ https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000022933195/2020-07-06/

¹⁵ http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Medical_Treatment_Law.pdf

video, email, smartphones, wireless tools, and other forms of telecommunications technology" (Glinkowski et al., 2018). The scope could be widened to the provision of "clinical care, education, public health, and administrative services at a distance" (HRSA in Lin et al., 2018).

Worldwide. Telehealth has been exhaustively described by the World Health Organisation as the "delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information" (Botrugno, 2019). As noticed by Otto et al. (2018), both terms can be distinguished based on the involvement of healthcare providers: telemedicine can be seen as a service exclusively delivered by physicians (WHO, 1997), while telehealth includes the delivery of services by all existing healthcare providers (WHO, 2010).

Furthermore, Sood et al. (2007), who reviewed 104 different definitions of telemedicine, stressed important differences in perspectives, pointing out the existing heterogeneity of the terminology: "telemedicine may range from simple e-mail-based store-and-forward technologies to complex remote surgical technologies". A scheme, mapping the definitions according to the different contexts, has been established within the study and 4 perspectives: (1) **Medical** with the mention of "providing healthcare services" and "practice of medicine"; (2) **Technological** with the indication of the technology's role as "the use of communication systems"; (3) **Spatial** with the "geographical separation of patient and doctor"; (4) **Benefits** addressing the issue of uneven distribution and shortages of medical resources.

mHealth

mHealth or mobile health is a sub-segment of eHealth and can be considered as the use of smart or mobile communication devices, such as smartphones and tablets, for provision of health and well-being services and information.

This definition is not legally accepted. However, the common characteristics between definitions which could legally lead to a common European definition of these terms. It is to be noted that some definitions do have more in-depth definitions of concepts, but overall, there is a lot of overlap.

European Union. The eAction¹⁶ defined mHealth as "the use of mobile communication devices in health and well-being services covering various technological solutions, which support self-management and measure vital signs such as heart rate, blood glucose level, blood pressure, body temperature and brain activity". The EAHP (European Association of Hospital Pharmacists) uses these terms within its definition of mHealth but without referring to well-being. Cortez et al. (2014) notes that these services of mHealth are defined broadly, encompassing diagnosis and management of conditions and support for general health, well-being and fitness. It is important to distinguish medical apps from well-being apps. Medical apps rely on applications that provide medical information. At the European level, the main regulation on mHealth apps is the Medical Device Regulation 2017/745, come into application in May 2021.

North America. The FDA (2016) includes in its definition of mobile health the "smartphone apps designed to foster health and well-being". The range of apps includes programs which "send targeted text messages aimed at encouraging healthy behaviours", "alert about disease outbreaks" or "help patients with reminders to adhere to specific care regimens". Increasingly, "smartphones may use cameras, microphones, or other sensors or transducers to capture vital signs for input to apps and bridging into RPM".

¹⁶ http://eaction.eu/wp-content/uploads/2021/01/eAction_D4.1_Policy-Framework-People-Empowerment_Final.pdf

Worldwide. The World Health Organization (WHO) defines mHealth as “medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices”. In 2011, the WHO Global Observatory for eHealth (GOe) defined mHealth as a component of eHealth. Although no standardized definition of mHealth has been established to date, the WHO GOe defined it as a “medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices” adding “mobile computing, medical sensor, and communications technologies for health care” to its definition (Catan et al., 2015). The field of mHealth is rapidly expanding as the global market for mobile devices grows. mHealth “apps” offer benefits and pose risks to users which governments have attempted to address through regulation. Otto et al. (2018) pointed out that mHealth is not a well-defined concept, highlighting the definition suggested by Nacinovich (2011) as “the use of mobile communications for health information and services” which, unlike telemedicine, is “possible without the direct involvement of health service providers”. According to Jogova et al. (2019), there are three ways in which services can be provisioned: “(1) software applications (“apps”) that allow users to enter and receive information, (2) pre-existing hardware (e.g., microphones, cameras) installed on portable devices and (3) external devices attached to portable devices that receive/generate information of interest (e.g., an attachment allowing a smartphone to read an electrocardiogram)”. Mobile health thus involves not only the use and capitalisation on a mobile phone’s core functionalities but also a more complex set of functionalities brought by software, monitoring and mobile devices.

2.1.2 Overview of the provision of digital health services and products on the market

The current trend of eHealth systems is “patient-centricity”, where the patient/consumer has to actively participate in his health management, backed by a dynamic environment of innovative consumer-centred services aiming at improving access to care and quality of care. eHealth puts an emphasis on prevention and empowering consumers in proactively managing their own health. From the health provider’s perspective, eHealth increases efficiency (locally, regionally, and worldwide) through the decrease of hospitalisations and lengths of stay and the avoidance of duplication of procedures; increases reliability and improves access to patient history. However, the “digital divide” gap is widening in western civilisations, not only due to a lack of access (first-level digital divide) but also due to a lack of use (second-level digital divide) (Griebel et al., 2018).

The use of eHealth products and services is driven both by consumers, who seek to take advantage of technologies that can improve their health and quality of life, and by healthcare systems. Some recent industry reports¹⁷¹⁸ estimated that Europe Digital Health Market share was valued at around EUR 43 billion in 2020 and is expected to witness a Compound Annual Growth Rate between 16% and 28% from 2020 to 2026, to reach around EUR 193 billion in 2026. This growth of the global e-health market is majorly driven by the increase in government initiatives supporting the use of e-health solutions and services, and the dearth of healthcare professionals in isolated areas, which pushes for the use of e-health solutions.

This market can be segmented by type, namely: Electronic Health Records, Archiving & Communications Systems, Laboratory Information Systems, telehealth, e-prescribing solutions, medical apps, clinical decision support systems, pharmacy, hospital information systems. It could also be segmented into different areas of services: (1) Remote care delivery; (2) Health data management; (3) Patient management; (4) Telemonitoring; (5) Diagnosis and therapeutic

¹⁷ <https://www.graphicalresearch.com/industry-insights/1163/europe-digital-health-market>

¹⁸ <https://www.marketdataforecast.com/market-reports/eu-e-Health-market>

decision; (6) Health information. The surge in adoption of smartphones, tablets, and other mobile platforms is driving the growth of the market and the medical apps segment is anticipated to grow with the largest share throughout the next years.

For costs and benefits analysis related to the harmonisation of practices, we considered the way eHealth contributes to the full spectrum of accessing the data and providing the care, including avoiding unnecessary travel, reducing redundancy and waste of resources, reducing intensity of care while minimizing adverse events, decreasing the time spent in consultation, decreasing the mortality rate and increasing patient satisfaction including: convenience, acceptability and willingness to use eHealth services in the future. We assessed such costs/benefits through 3 levels of costs ("‐": low costs, "‐‐": medium costs, "‐‐‐": high costs) and three levels of benefits ("‐+": low benefits, "‐‐+": medium benefits, "‐‐‐‐": high benefits). For each research area, the drivers and obstacles have been addressed in a synthetic table providing this analysis. For a driver, the cost is related to the resources needed to harmonise the rules, for an obstacle, the costs represent the negative impact for the stakeholders for not harmonising the rules.

The 2018 market study on telemedicine¹⁹ provided with a decision model for economic assessment, which could be reused by adapting the parameters to encompass all eHealth services. For instance, it could consider lower costs (e.g. 10% to consider the use of less expensive technologies), increased success rate (e.g. 5%) or decreased mortality rate (e.g. 10%) to consider more efficient devices, as quantitative benefits. Additional costs would be evaluated and compared to the current system of delivering health care. However, these assumptions will remain highly dependent on an evaluation of the current market and practices, including a quantification of current practices (e.g. how much those products and services precisely represent within the current market).

However, in the next chapters of this report, the focus has been made on some of these services, mainly given the inputs and insights provided during the consultation, namely: telemonitoring, health data management and more broadly health apps. Following the previously analysed definitions, the following table gives an overview on the way these digital health services are defined.

Table 2. Overview of definitions

Area	Objectives	Services
Remote care delivery	Remote care delivery services aim at providing clinical health care where the parties involved are not in the same location	Teleconsultation, tele-expertise (e.g. telesurgery, teleophthalmology, teleradiology, tele-dermatology, etc.), and remote medical assistance, through asynchronous communications, synchronous real-time communication (live video, etc.) between patients/health professionals or between professionals/professionals
Health data management	Health data management is intended to facilitate the exchange of patient data between health care professionals and patients. The objective is to improve the interaction between patients	Patients' EHR (Electronic Health Records) and digital patient summaries, often implemented nation-wide, patient data portals or personal health data spaces Services providing secure storage and/or secure transmission of medical data with information such

¹⁹ https://ec.europa.eu/health/sites/default/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf

	and health-service providers or professionals and the institution-to-institution transmission of data in order to speed-up procedures	as text, sound, images and other types of data (which is needed for the prevention, diagnosis, treatment and follow-up of patients).
Patient management	Patient management revolves around maintaining the continuity of care and with the administrative and medical follow-up of patient/public health issues.	ePrescription (electronic transmission of prescriptions, remote renewal of medicines), eReferral tools, automated pricing systems, reimbursement/billing/claims management tools, and medical appointments management tools, instant or asynchronous secure messaging systems/apps
Health information	Health information availability may improve both patient and professional health-related education, by providing valid, widely understandable and available information. This area aims to continue health-related education of patients and health care providers and to facilitate knowledge exchanges to improve prevention through the exchange of valid information.	Patient forums, health information pages and portals (providing health literature, health education, knowledge and research), call centres/online information centres for patients, patient and professional health related education, public health and health administration, educational sessions. These services could use mHealth monitoring apps to produce alerts about disease outbreaks or text messages aimed at encouraging healthy behaviours, helping patients with reminders to adhere to specific care regimens/programs

Source: Authors' elaboration

2.1.3 Current EU MS national practices and cross-border provision

The 2011/24/EU cross-border Directive sets the conditions under which a patient may receive cross-border healthcare in other Member States and be reimbursed for it and is meant to define the entire scope of cross-border healthcare services, including digital health services. The Directive provides guidance on the scope of reimbursement, patient information and mutual recognition of prescriptions. Both human health protection and patient mobility are key issues to cross-border care. Besides, the ethical challenges of the Cross-border Healthcare Directive should also be considered when assessing its implementation among Member States (Olimid, 2019).

Scope of reimbursement. The 2011/24/EU Directive covers situations where a patient is provided with healthcare in a Member State of Treatment (MST) other than the Member State of Affiliation (MSA), along with the prescription, dispensation and provision of medicinal products and medical devices in the context of a cross-border healthcare service. As for telemedicine, the Directive 2011/24/EU states that healthcare is considered to be provided in the Member State where the healthcare provider is established, Member State of the provider. Only healthcare provided in the MSA is not covered by Directive 2011/24/EU, as in such a case, there is no cross-border element. Healthcare services and products are covered by the TFEU articles on free movement of services and goods. The concepts defined in the previous section do not entirely appear in the definition of telemedicine provided in the Directive, as it does not include for instance telemonitoring systems and mobile health, stressing a potential gap to be able to regulate such products and services (e.g. non-medical apps). The focus has been made on such products and services in this report to clarify their scope. Article 56 TFEU also applies to digital healthcare services. However, Article 1 states that "this Directive shall not affect laws and

regulations in Member States relating to the organisation and financing of healthcare in situations not related to cross-border healthcare". Indeed, nothing in the Directive obliges a Member State to reimburse costs of healthcare provided within its internal healthcare system. Article 4 takes "into account the principles of universality, access to good quality care, equity and solidarity" and points out that "cross-border healthcare shall be provided in accordance with the legislation of the Member State of treatment". Moreover, Regulation 883/2004²⁰ on the coordination of social security systems sets up the basis of reimbursement at cross-border level by harmonising the conditions and field of applications of reimbursement. Some healthcare services and products should be reimbursed according to this regulation, such as sickness, maternity and equivalent paternity benefits. This regulation also set up the basement of prior authorisation for planned care (article 20). The Regulation 883/2004 implies mechanisms within the field of coordination of social security systems and confirms that such rules fall within the framework of free movement of persons, adding through Article 35 that "the benefits in kind provided by the institution of a Member State on behalf of the institution of another Member State shall give rise to full reimbursement".

Patient information. According to 2011/24/EU Directive, the cross-border healthcare shall be provided in accordance with the MST's safety and quality standards. Germany provides more information to patients than in Article 5: treatment data, diagnosis, implications for health condition, treatment and follow-up measures, therapy options and estimated costs of the service.

Data portability. The eHDSI, set out on the basis of Article 14 of Directive 2011/24, supports sending data from MSA to MST, at the request of the patient, to be made available to health professionals. However, this does not allow citizens (not necessarily patients) access their own data across borders. The Directive does not set out any rights of individuals to access/control their health data generated across borders (or nationally), neither through the MSA or MST. This is identified as a gap, which prevents the Directive from covering the case of remote health data accesses.

Authorisation of treatments. According to 2011/24 Directive, healthcare subject to prior authorisation shall be limited to healthcare (a) subjected by planning requirements to guarantee quality of care for citizens of the MST (overnight hospital accommodation or highly specialised and costly equipment), (b) involving particular risk to the patient or population or (c) with specific risk related to quality or safety of the provision. There are only 4 reasons an MS can refuse to grant prior authorisation.

Mutual recognition of prescriptions. The 2011/24 Directive states that if a prescribed medicinal product is authorised to be marketed in the Member State, then the product shall be delivered to the patient, based on a prescription issued in another Member State. According to article 3(k) of Directive 2011/24/EU, a 'prescription' is "a prescription for a medicinal product or for a medical device issued by a member of a regulated health profession within the meaning of Article 3(1)(a) of Directive 2005/36/EC who is legally entitled to do so in the Member State in which the prescription is issued".

However, some Member States, such as France, states that the dispensator can refuse to deliver the medical product in case of justified doubts on authenticity, content or intelligibility of the prescription. It thus leaves to professional judgement to determine whether the product is suited and to recognise the prescribing professional's qualifications.

²⁰ [EUR-Lex - 32004R0883 - EN - EUR-Lex \(europa.eu\)](http://EUR-Lex - 32004R0883 - EN - EUR-Lex (europa.eu))

Lastly, it should be noted that the 2011/24 Directive applies in European Union since 2013 and in the European Economic Area (Norway, Iceland, Liechtenstein) since 2015. Switzerland is not affected by this Directive. However, the EHIC (European Health Insurance Card) could be used both in the European Economic Area and in Switzerland.

Box 3. Examples of European cross-border telemedicine projects

Below are some relevant examples of currently running telemedicine initiatives in a cross-border context, used to illustrate the implementation of digital health practices across Europe.

- **Pomerania project**²¹ is mainly funded by the European Commission (up to 84%) and involves 20 German and 15 Polish hospitals. It aims at enlarging the healthcare services offered in a region with a low density of hospitals and covers fields such as radiology, urology, stroke care, cardiology, oncology, ophthalmology, ear, nose and throat illnesses.
- The **European Stroke Organisation** is a Swiss organisation bringing together European stroke experts and aims at improving the delivery of stroke services. They produce guidelines²² for the implementation of a tele-stroke network in Europe in a practical way.
- The university hospitals of Aachen (Germany) and Maastricht (the Netherlands) share the services of one neurophysiologist, through the use of telemedicine practices for certain procedures. Surgeons are able to operate on a patient at Aachen Hospital while the neurophysiologist in Maastricht follows the operation on a screen and monitors the patient's condition.
- In 2006, Denmark and Sweden started a telepsychiatry collaboration for asylum seekers and migrants. Only one Danish hospital had a cross-cultural expertise (Mucic 2008) and the study showed a good acceptance of patients towards telemedicine and an appreciation to exchange with a healthcare professional without an interpreter.
- A shared software platform has been created between France and Swiss in order to establish collaborative diagnosis, to study neuroimaging, as well as to access virtual examination. A virtual network is even used to transfer diagnosis from university hospital Basel to collaborating German district hospitals.

However, it is important to stress the fact that the cross-border initiatives identified above are generally located in small border regions, funded by the European Union, specialised in a specific therapeutic area and often poorly documented.

Source: Authors' elaboration

²¹ https://ec.europa.eu/regional_policy/en/projects/germany/telemedicine-pomerania-improves-healthcare-in-sparsely-populated-regions

²² <https://www.telemedecine-360.com/wp-content/uploads/2019/03/2018-ESO-Recommendations-on-telestroke-in-Europe.pdf>

Box 4. The European University Hospital Alliance (EUHA)²³

The European University Hospital Alliance gathers nine of the leading university hospitals in eight Member States (Austria, Belgium, Germany, France, Italy, Netherlands, Spain, Sweden, United Kingdom) and aims at improving healthcare outcomes for patients through fostering innovation, research, education and excellence. The EUHA implemented the digital Platform for Procurement of Innovation and Innovation of Procurement²⁴ (PIPPI), launched in 2020 and supported by H2020. It is intended to bring together expertise on digital healthcare, patient-centred care and procurement from the demand and supply angle by assessing and addressing common unsolved challenges (both clinical and legal) concerning health innovation, digital care and data exchanges. The main objectives are to:

- Establish, leverage, and scale a shared set of tools and practices for the common benefit of healthcare providers, patients/citizens, private sector, and policymakers;
- Establish an open access web-platform for multi stakeholder communication and collaboration.

Source: Authors' elaboration

2.2 Fostering cross-border digital health: drivers, obstacles, costs and benefits

2.2.1 Background

In order to foster a single market for digital health, several topics should be addressed, firstly by identifying the drivers supporting its cross-border provision of such products and services and the obstacles hindering their use.

The approval, certification, authorization and reimbursement of digital health products and services rely on processes and schemes set out by Member States at national or regional levels. EU action must respect the responsibilities of Member States for the definition of their health policy and for the organisation and delivery of health services and medical care²⁵. Thus, although the EC has a coordinating role, its room for manoeuvre is limited and it cannot directly harmonise the benefits to which citizens may be entitled. However, a harmonisation of healthcare access across the EU would be one of the benefits for cross-border healthcare expected from a regulation of digital healthcare. Through the eHN, various initiatives (e.g. Joint Actions) have been taken to promote cooperation at EU-level in this area.

Interoperability has long been identified as a key issue in facilitating data exchanges between healthcare providers, patients and institutions, dealt with several regulatory measures and initiatives. Some obstacles are still preventing Member States from developing an efficient cross-border interoperability of eHealth services and products.

Following the entry into application of the GDPR, data protection will be a key issue to embed in digital health products and services in order to build trust in a cross-border setting. The Directive 2011/24/EU on Cross-border healthcare provides only few direct mentions of safety, privacy and consent issues: these aspects are mainly introduced within Article 4 of Chapter II. More specifically, Article 4 refers to other directives applicable in the field of health data protection. However, privacy and liability cover key aspects of digital health, especially through ePrescription and data shared from EHR.

²³ <http://www.euhalliance.eu/about-the-alliance/the-alliance/>

²⁴ <https://pippi.meduniwien.ac.at/>

²⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008E168>

Professional qualifications are a key issue in digital health, given that the services are usually used without the physical presence of the professional. Healthcare providers must therefore be sufficiently skilled and qualified to provide such distant care: they must be able to master the tools and provide support to the patient in its understanding and its use.

The potential added value provided on ePrescription brought through the data spaces also has an impact on the sale and the delivery of on-prescription pharmaceutical care to outpatients at a distance, as an extension of brick-and-mortar pharmacies.

2.2.2 Approval, certification, authorisation and reimbursement

Drivers

Common assessment practices. Not all Member States are on the same page when it comes to eHealth reimbursement practices. Without any doubt, the differences between healthcare systems play an important role in it. For instance: while the Netherlands' liberalisation since 2006, implied there hasn't been central steering in defining healthcare standards, France has a central decision making with processes to implement locally such decisions and Italy relies on a delegation of reimbursement decisions at a regional level. In France, comparative clinical evidence and budget impact drive reimbursement decisions in terms of pricing and restrictions, whereas in Italy, regional key opinion leaders (KOL) have support roles and local observational data is key to the reimbursement decisions (Schaefer et al., 2015). Thus, when analysing differences in eHealth reimbursement practices within Member States, the main distinctions are (i) between the Bismarck model of social insurance and the National Health Services systems (ii) within NHS systems, the degree of central/regional autonomy of policies and funders.

Box 5. EUnetHTA, a cooperation on eHealth technology assessment towards common schemes

As stated by article 15 of the Directive, "the Union shall support and facilitate cooperation and the exchange of scientific information among Member States within a voluntary network connecting national authorities or bodies responsible for health technology assessment designated by the Member States". It should be noted that proposals on HTA Regulation are still pending and will replace Article 15 through a separate legal act.

Health systems have a vital role across the EU in the coordination of shared evaluation criteria. While the market approval procedures for Medical Devices are uniform in the EU Member States, this is still not the case for eHealth technology when solutions do not fall under Medical Devices Regulation. From a regional perspective, eHealth technology assessment schemes are fragmented and would benefit from standardization, as currently carried out on interoperability.

The formal launch of the "EU-wide network on HTA (EUnetHTA)", which focuses on the collaboration and exchange of information on HTA (applied criteria, methodology, research outcomes, among others), has been a first step towards further collaboration. Such action is intended to prevent the duplication in HTA research of new technologies and to help less experienced countries to make transparent and well-balanced health policy decisions. The EUnetHTA Joint Actions spread "best practices" and methodology guidelines whereas the EUnetHTA's HTA Core Model is an important tool for standardising and sharing HTA information based on a methodological framework which identifies nine research domains (den Exter et al., 2015): health problems and current use of technology; description and technical characteristics of technology; safety; clinical effectiveness; costs and economic evaluation; ethical analysis; organisational aspects; social aspects; and legal aspects.

Source: Authors' elaboration

There are already many challenges in the evaluation of clinical effectiveness of Medical Devices, deriving from the physical mode of action, the incremental development, the context dependency or the different market environments and regulatory requirements (Schnell-Inderst et al., 2015). The aim of digital health assessment should not be to reduce evaluations or to increase their depth but rather to adapt to the special nature of digital health. There could be reference to "hard" end points, such as mortality, morbidity and quality of care, as well as "soft" criteria, such as autonomy or gain in comfort, although these are partially used in a quality of life assessment (Albrecht, 2018). A standardised evaluation approach would be based on the value delivered by digital health solutions (clinical, organizational, behavioural and technical). These evaluation tools could be used by weighing different attributes and criteria in terms of how beneficial and important they are (Kolasa et al., 2020).

Currently, only part of this assessment is taken into account by the Netherlands and several other European countries, where most HTAs use QALYs in cost-effectiveness analyses (assessing life expectancy and quality of life at the same time), but ignoring the organisational and technical input. . The majority of HTA studies focus on newly developed medicines rather than other medical technologies (den Exter et al., 2015).

The absence of RCTs for devices is part of the challenge faced by HTA studies. Lastly, when looking at the economic analysis of ehealth solutions, it is important to take into account the nature of these solutions, which are intended in particular to produce data that will have to be fed into health systems. Thus, many digital integration costs must be taken into account (notably: interoperability, cybersecurity, data protection, identification/authentication, etc.), yet these costs are not fully taken into account at present in reimbursement decisions. This is one area where digital health bodies could provide expertise.

Outside the EU, the NHS issued Digital Guidelines²⁶ on health apps and digital tools assessment, providing general guidance on how to define criteria, whereas the FDA issued six different regulatory guidelines related to Software as Medical Device (SaMD), Software in a Medical Device (SiMD), Clinical Decision Support Software, and others^{27,28}.

²⁶ <https://digital.nhs.uk/services/nhs-apps-library/guidance-for-health-app-developers-commissioners-and-assessors/how-we-assess-health-apps-and-digital-tools>

²⁷ <https://www.fda.gov/medical-devices/digital-health/guidances-digital-health-content>

²⁸ <https://www.fda.gov/media/80958/download>

Box 6. «CE» marking for medical devices

The CE marking is a label certifying that a specific product complies with the European legislation. It applies to any product designed for a European distribution, especially medical devices. It can be delivered by a notified body, accredited body performing conformity assessments for medical devices²⁹. The specific assessment procedure involves three main steps³⁰, namely:

- The evaluation of the technical documentation, including clinical trials and consulting the EMA (European Medicines Agency) for its scientific approval;
- The on-site audit for assessing the system for quality management;
- The production of a detailed audit report.

A Medical Device is “any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes detailed in Article 2 of the Medical Device Regulation” (MDR or Regulation 2017/745/EU³¹). It is classified in accordance with the provisions of Annex VIII of the Regulation 2017/745/EU as class I (low risk), class IIa or IIb (medium risk) or class III (high risk). It should be noted that the involvement of a Notified Body is not necessary for medical devices of class I unless they have a measuring function or are placed on the market in a sterile condition³². Software, and thus eHealth products and services, also fall within this legal framework, often being considered as class IIa Medical Devices.

Source: Authors' elaboration

Quality labelling. Many stakeholders (international public organisations, eHealth experts, patients representatives, professionals representatives and industry representatives) consulted during the study expressed their interest in an EU-level labelling as well as in quality assessments for eHealth products and services. According to European patients' representatives, labelling is not only an example of providing easily accessible and readable information to citizens, but also of empowering citizens to better understand the use of their health data. It was stated during the consultation that accountability and transparency are key elements for trust in quality labels (e.g. healthcare professionals will not prescribe a service that is not certified or reimbursed). In order to increase trust in digital health devices, mHealth technologies could benefit from being endorsed by a doctor, most trusted actor in health care. Several eHealth experts added that the surest way to drive this process would be for the doctors to be able to prescribe and for the product/service to be reimbursed as a medicine, medical service or device. In addition, labels can cover different scopes: medical devices, non-medical devices, mobile apps, digital devices, etc. Three main objectives were identified for such a labelling through the use cases of the consultation: (i) **inform patients and users** on trustworthy healthcare applications and digital services by “stamping” services on publicly available marketplaces, (ii) **foster adoption** among healthcare professionals, especially with the inclusion of testing benches for healthcare professionals which will enable them to deeply trust the technology, (iii) **support decision making** for notified bodies or Health Technology Assessment bodies among Member States and thus building trust for end-users and creating transparency on the reimbursement decision-making (labelling could also be a repository of labelled/assessed apps).

One-time certification should not be the modus operandi to ensure labelling of digital health services. Both the re-evaluation of solutions and the monitoring of certifications are vital to the

²⁹ <https://www.ema.europa.eu/en/glossary/notified-body>

³⁰ <https://certification.afnor.org/qualite/dispositifs-medicaux>

³¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02017R0745-20200424>

³² https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en

well-being of the labelling system. An eHealth expert mentioned that including new criteria (such as interoperability) in quality labels would lead to the “re-certification” of medical devices already on the market. Although this would be difficult and costly in the short term for the producers, the long-term advantages gained from streamlining such a certification process would be significant, especially when dealing with liability and interoperability issues that could arise.

Although several quality criteria have already been suggested through European initiatives, including for mobile health assessment (see *in section 3.2.2.4: Existing mHealth frameworks, assessment guidelines and code of conducts*), still very few apps or solutions can be found on existing repositories. There is a need for more efficiency at an EU level, since labelling can act as a lever for their use. Besides, national institutional stakeholders mentioned the importance of including data quality for care safety in such labelling. Among the possible quality criteria to be included in such an assessment have been cited by international public organisations stakeholders, among others: technical requirements (data storage, data transmission, security standards, data quality, UX design...), public health issues (care quality and safety, accessibility...), policy regulation (consent, access to information, compliance, liability). The French Health Authority issued Good Practice guidelines on health apps and smart devices assessment³³, including as areas: Informing users, Health content, Technical content, Security/Reliability, Usability/use.

Innovative access pathways. According to stakeholders from the consultation, the key conditions that should be considered in the reimbursement of digital health tools are the clinical benefits and the cost saving aspects of the tools, outlining that the patients are expecting health care products to be reimbursed if they show positive outcomes on their health. According to some national institutional stakeholders, digital health services should follow HTA national processes before European processes, however eHealth and innovative products specificities could be included since the current HTA processes focus on quality of care. Several Member States laws already cover experimental services and innovative access pathways for digital health, such as **mHealth** in Belgium, **DiGA** in Germany, **Article 51** in France. Fair models are still eagerly awaited to be set-up in order to support developing SMEs' opportunities and to reduce the difficulties they face when entering the market. One way to support such access to innovation would be the lowering of barriers to national or regional markets entry, with harmonised requirements resulting in fewer customisation efforts. Besides, this would lead to better offerings and lower costs of digital health solutions.

Existing mHealth frameworks, assessment guidelines and code of conducts. Many of the stakeholders involved mentioned that the value of a mobile health app lies not only in app quality (for 20%) but also in how the app is used and is integrated in health and care processes (for 80%). Similar or harmonised requirements amongst MS and often even regions, would promote the scale-up of mHealth solution providers. This would strengthen the business case for mHealth developers. Several references were made to the German **DiGA** law setting-up a fast track certification and reimbursement scheme for mHealth apps (see Annex 7.6 for an analysis of assessment frameworks). This model stimulated innovation in the mobile health field in Germany despite the rather conservative nature of the country on data sharing. Nevertheless, although several health applications are being reimbursed through this innovative process, it is still perceived to a certain extent as a “black-box”. Belgium has developed its own certification process through the **Belgian mHealth** platform, defining three

³³ https://www.has-sante.fr/upload/docs/application/pdf/201703/dir1/good_practice_guidelines_on_health_apps_and_smart_devices_mobile_health_or_mhealth.pdf

levels of certification for mobile health applications, supporting the analysis of the potential impact on their use and managing a schedule of applications maintenance.

Box 7. Report of the Working Group on mHealth Assessment Guidelines (2017)³⁴

Following its creation on February 2016, the stakeholders' Working Group on mHealth assessment guidelines concluded its work through a report published in July 2017³⁵, a work intended to develop guidelines for assessing the validity and reliability of the data collected and processed by health apps. Following the interest in broadening this scope, members of the Working Group were invited to give their views on 13 selected assessment criteria, namely: privacy, transparency, safety, reliability, validity, interoperability, technical stability, effectiveness, efficacy, efficiency, accessibility, usability, and scalability. The different views were split into six stakeholders' constituencies: Patients, Healthcare Professionals, Industry, Public Authorities, Payers and Research. Even though no guidelines were achieved nor endorsed, an identification of case studies and existing guidelines has been carried out, providing a tangible base for further work and regulation on the matter.

The responses showed a consensus view on the **relevance of six assessment criteria**, namely: (1) Privacy, (2) Transparency, (3) Reliability, (4) Validity, (5) Interoperability and (6) Safety -with the exception of the industry representatives' opinion who chose to limit their feedback to address data validity and reliability as initially foreseen by the mandate of the group-. Although Patients, Healthcare Professionals and Payers also agreed on the increased relevance of effectiveness, a disparity was identified in the understanding of this term. Payers stated that "all users of the target group of an app must be able to use it: in case there are limitations, the app should make them transparent, e.g. for persons with low vision". Industry considered usability as a market-related issue, and the patients representatives suggested two additional criteria: user experience/design/suitability and security.

Source: Authors' elaboration

It seems particularly important to be able to map the entities involved in the mobile apps market to the entities defined within the European regulatory framework, as well as to increase the awareness about the medical regulatory framework by promoting education initiatives for all the players involved in the development and commercialization of mobile medical apps (Censi et al., 2015). Indeed, such a mapping will help regulation, considering the increasing amount of 'well-being' apps that most will not be classed as medical devices. On the matter, the FDA has shown a pragmatic approach (Quinn, 2017): it uses a risk-based approach with a case-by-case look at apps that may or may not be medical devices (such as well-being apps).

³⁴ <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3390&NewSearch=1&NewSearch=1>

³⁵ http://ec.europa.eu/newsroom/document.cfm?doc_id=45251

Box 8. Quality criteria: standards ISO/CEN 82304-2

At the request of DG CNECT, CEN and ISO are working towards standards on eHealth assessment criteria under this standard split into five areas, including quality aspects: (1) Medical safety, (2) Usability, (3) Security of personal data, (4) Technical quality, (5) Quality of the app. This work is guided by other frameworks and studies' questions about health and safety, health requirements, ethics, health benefits, societal benefits, health risks, accessibility, privacy and security, and interoperability. This work could especially be used to support labelling at an EU level.

The Dutch Ministry of Health has commissioned the National eHealth LIving Lab (NeLL, Leiden University Medical Center) to build a national health app assessment framework based on CEN-ISO 82304-2 and to advise how to execute such a framework. A comparative study has been led on several app assessment frameworks, including those from Haute Autorité de Santé (France), mHealth Belgium, DiGA (Germany), Digital Technology Assessment (United Kingdom) and existing Dutch frameworks. The aim was to establish which requirements overlap with CEN-ISO and which are not yet covered in CEN-ISO and should be considered as additional Dutch requirements, and significant overlaps have been found in subjects covered. It concludes that CEN-ISO standard covers the national requirements well, with a few exceptions.

Source: Authors' elaboration

The **European Innovation and Knowledge mHealth Hub** is a combined initiative between the WHO, the ITU and the Andalusian Regional Ministry of Health, funded by the European Commission. Its main objective is to allow countries to benefit from other countries practical experiences by offering a basis for researchers, project coordinators, experts and technical support teams to develop knowledge, capability and technical expertise in a specific field.

Box 9. mHealth Hub framework³⁶ and use cases

Six work areas to be addressed have been identified: (1) mHealth assessment frameworks, (2) Evidence-based mHealth solutions on NCDs, (3) Integration of mHealth into health systems, (4) Support for large scale implementation of mHealth programmes, (5) Contributions to policy frameworks on mHealth topics and (6) Ethics.

In 2020, a first tool was developed: a Health apps assessment framework³⁷ to be approved by the European Commission, defining recommendations on the criteria for health apps assessment, health apps repositories and the major implications for patients. 14 technical recommendations have been issued, targeting several types of stakeholders. Two relevant examples were annexed to the report of the Working Group to be used for legislation guidance as case studies:

Andalusian mHealth strategy: in 2012, the Andalusian public health system defined its own "Recommendations for the design, use and evaluation of health apps"³⁸, 31 recommendations and subsequent requirements split into 4 sections: (1) "Design and appropriateness" (accessibility, design and usability), (2) "Quality and safety of information" (suitability for the audience, transparency and authorship, information update, content and information sources, risk management), (3) "Provision of services" (technical support, e-commerce, bandwidth, advertising) and (4) "Confidentiality and privacy" (privacy and data protection). These recommendations support the Appsaludable Distinctive³⁹, launched in 2013, as the first quality seal for health apps in Spain. The seal is based on a self and external assessment methodology. Since 2013, more than 150 apps have been assessed.

Medappcare is the first European private organisation which has developed a rigorous and independent multi-criteria reference tool for assessing mobile health applications. It places itself as a trusted third party in assessment and approval, carried out at the developers' request. Its assessment includes 70 criteria, split in 4 main assessments : (1) "Regulatory and legal assessment" (data protection, GCU accessible, application objective aligned with regulation and ethics, obtention of user consent, targeting advertising), (2) "Technical and security assessment" (functionality, viruses or malicious software, access to local resources, risky network connections, securing personal and health data exchange and storage), (3) "Medical assessment" (adapted content, reliable information, respect of ethics, developer's legitimacy and competences) and (4) "Ergonomics and usability assessment" (data portability, interoperability, support, intuitive and easy to use, complete and adapted help system, information design and legibility, usability, usefulness).

Source: Authors' elaboration

Furthermore, another proposal similar to the Andalusian strategy has been highlighted as an insightful initiative during the consultation: a dual-factor certification where the developer would be able to self-certify the app on a first level (self-certification declarative process). Such an assessment could be carried out through the criteria covered by a code of conduct. Then, a national/regional entity would approve the self-certification and review the compliance on other criteria, providing a certification label. Two main models could be found for the entity providing the certification: either a federated model including independent bodies with distributed roles or a centralised model where the government provides the necessary bodies and guidelines.

Lastly, the European Commission, drafted a code of conduct for the development of mobile health apps. At the time, this work was carried out in a tense context, where it was quite difficult

³⁶ <https://mhealth-hub.org/mhealth-hub>

³⁷ <https://mhealth-hub.org/download/d2-1-knowledge-tool-1-health-apps-assessment-frameworks-pending-ec-approval#>

³⁸ http://ec.europa.eu/newsroom/document.cfm?doc_id=45253

³⁹ <http://www.calidadappsalud.com/en/>

to assess the entire scope of apps that were being produced. Although defining an assessment seemed challenging, the issues to be covered by the code were decided, namely: (1) User's consent, (2) Purpose limitation and data minimisation, (3) Privacy by design and by default, (4) Data subjects' rights and information requirements, (5) Data retention, (6) Security measures, (7) Principles on advertising in mHealth apps, (8) Use of personal data for secondary purposes, (9) Disclosing data to third parties for processing operations, (10) Data transfers, (11) Personal data breach, and (12) Data gathered from children.

Data evidence availability to support decision-making in cross-border care. The Article 9(2) of the Directive states that "any administrative procedure [...] shall be easily accessible and information relating to such a procedure shall be made publicly available at the appropriate level". Moreover, the article 9(3) adds that "Member States shall set out reasonable periods of time within which requests for cross-border healthcare must be dealt with". However, these conditions are administrative procedures regarding the use of cross-border healthcare and reimbursement, which do not have direct implications regarding access to databases across MSs and authorising data access or accessing data for reimbursement purpose. It should be noted that in the USA, an effective exchange of data is "still necessary to drive appropriate reforms on delivery and payment nationwide for eHealth services" (Gold et al., 2016).

Besides, the current trend in Europe shows an increasing use of patient-reported outcome measures (PROMs) to demonstrate the value of devices. Consequently, the need for available evidence is surging, to support decision and meet country-specific requirements for authorisation or reimbursement. One important point brought up during the consultation was the necessity to avoid slowing-down the authorisation process, especially for SMEs, or any overlapping between existing certification processes. It appears thus vital to centralise and harmonise the collection of information used for decision making purposes. The current work on the ISO/CEN 82304-2 standard aims precisely at providing this information not only through a technical label but a quality label, to help narrowing the decision-making process.

Existing EU governance on assessment issues. The consultation showed that some stakeholders groups such as industry representatives, e-Health experts and healthcare professionals representatives agree that the existing bodies and networks (HTA Network set up by Directive 2011/24) are a solid basis to support assessment of digital health products, in order to structure and monitor a common European standardised evaluation model, with specific bodies contributing to the decision. There is no existing common European framework in the field, since the only applicable legislation is Council Directive 89/105/EEC of 21 December 1988, relating to the transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of national health insurance systems. Although defining of baskets of benefits is MSs competence, such an organisation could leverage the support to Members States in their reimbursement decisions. On January 31st, 2018, the European Commission released a proposal for a new regulation on HTA cooperation⁴⁰, aiming to streamline disparate national HTA processes and generate a single, joint clinical assessment, with a focus on joint relative effectiveness assessment (REA) of pharmaceuticals and certain types of medical devices. A common initiative on the field of digital health could rely on such cooperation. eHealth experts highlighted during the consultation that the IHE Conformity is already carrying out interoperability testing and certification for eHealth services, also stating that the Commission could help pushing Member States to rely on private bodies to support public bodies.

However, European officials stressed during the consultation that digital tools assessment is under structuration worldwide, and the absence of a Single Market for digital health still hinders

⁴⁰ https://ec.europa.eu/health/sites/health/files/technology_assessment/docs/com2018_51final_en.pdf (2018)

the European scale-up of services and products. One running issue being that mobile health is a very large field for which no single body or institution consider having the required competencies to take full responsibility (with an understanding of both the medical and the technical implications). Some institutional stakeholders highlighted that HTA bodies currently measure technical quality and readiness for every health tool, not the organisational readiness of the organisations or systems (including interoperability, cybersecurity, identification, etc.) in which these tools and services must be integrated. It was also stressed that the cross-border context was the main difficulty at an EU level rather than digital aspects, which can be assessed with national processes. The need for practical guidance targeting healthcare professionals and developers to supplement the MDR (Medical Devices Regulation) was highlighted by the industry, to ensure that the products which can be part of telehealth services have the right level of clinical evidence, without a need for additional regulation.

European organisations such as the European Patients Forum wish for a better inclusion of patients in the certification processes or the creation of a labelling system for digital health tools. Such an inclusion would be very valuable to garner patients' trust in digital health tools, also benefiting the service providers, since patients remain the final users of many digital health services. According to their representatives, healthcare professionals generally face difficulties in recommending the best mobile health application to their patients because they are not able to assess properly how such services were developed, nor their trustworthiness or efficiency. Besides, the wide range of applications available on the market makes their advice even more complex. Professionals' organisations and industry representatives consider HP could be more involved in this process, since it remains up to the healthcare professionals, for each specific patient case, to judge whether an eHealth service is beneficial for the patient's health outcome.

Obstacles

National fragmentation of health systems, financing and reimbursement models. It has been outlined that the scattered frameworks and reimbursement mechanisms are not driving towards a harmonisation of assessments. Reimbursement is subject to national law and is highly dependent on national, regional or local healthcare systems. As a result, there are significant differences in the regulation that may or may not apply to software, in addition to the MDR. Furthermore, rules which are not mandatory per se could be a condition for financing or reimbursement. The mobile health market remains especially fragmented at the EU scale: not one single app is approved for reimbursement in more than one country. One important question revolves around whether digital health solutions should be funded by the public budget, as other health technologies. The grounds for this discussion are that digital health solutions can bring at least two types of benefits: (1) clinical gains achieved by a more effective treatment, or (2) safe treatment and efficiency gains achieved by a better organization of the healthcare system (Kolasa et al., 2020).

However, in countries where eHealth isn't well developed, local funding and reimbursement schemes still need to be created, especially for electronic devices. Even more important than the countries frameworks specificities or diversity is the current lack of reimbursement for digital health services. However COVID-19 pandemic had a huge impact on this matter, countries such as Austria, Belgium, Estonia and the Czech Republic that did not define jurisdiction, liability or reimbursement of services like telehealth, have since allowed provider payment for some telehealth consultations and clarified regulations⁴¹. Reimbursement and HTA systems for digital health in most of the Member States aren't well developed, not covering digital health

⁴¹ https://ec.europa.eu/health/sites/default/files/state/docs/2020_healthatglance_rep_en.pdf

technologies that deliver cross-border services. Furthermore, since no legislation directly addresses the mobile health environment and no certification assesses either trustworthy apps or the clinical methodology, it remains unclear for developers to identify specific supportive bodies. The consultation showed that health authorities and payers should prioritise the establishment of clear frameworks for reimbursement regarding digital health solutions. For practical purposes, reimbursement practices should rely on HTA.

An effort is needed to implement medical device regulations to the Mobile app Market (Censi et al., 2015) and further regulatory steps should be considered to simplify and extend reimbursement rules for eHealth applications, at the national level. Two examples have been given to illustrate rules which can be obstacles to access to innovation, without being a regulatory gap per se: the French Health Data Hosting certification requirement for patient data hosting or the Dutch hospitals requesting compliance with NEN Standards, which are 'Dutch only', and slightly different from ISO 27001. The industry representatives stressed the additional requirements and the involvement of heavy administrative processes to enter a specific market.

Lastly, fragmentation is also translated into inequalities in access to technology thus to eHealth (the "digital divide"), with disadvantaged populations considering the disparities of infrastructure and services between Member States. However, underserved populations should benefit from eHealth applications to generalise accessible healthcare (Ahern et al., 2006).

Box 10. Case studies – Bringing eHealth innovations into the market⁴²

A study from the "Allied for Start-ups" Belgian network analysed the impact of the Covid-19 pandemic on the teleconsultation market, based on six case studies of telemedicine start-ups. The main outcome is the raise of teleconsultation adoption for both the patients and doctors among European countries, as several decided to allow and reimburse teleconsultation and tele-expertise.

However, the lack of transparent regulatory framework and reimbursement schemes hampers the access to the public healthcare market for companies, especially public healthcare systems. Furthermore, this shortcoming is widening the gap between public and private healthcare as well as between large companies and start-ups. As an example, France tackled these barriers by setting-up a 350€-per-year financial support for doctors to buy hardware and provide eHealth services. As this initiative is still new, it is difficult to measure its impact today. However, we have observed an encouraging trend over the three years of operation, with a growing number of professionals eligible for this package

The study suggests that national bodies should keep an up-to-date impartial list of eHealth start-ups and companies to support healthcare providers in the adoption of telemedicine tools. The consortium also stated that ePrescription and EHR are the first two steps before developing digital health tools. However, the European legal frameworks need to go further in order to support innovations. For now, the regulations remain unclear and lack transparency, not only on telemedicine but especially on AI and machine learning.

Source: Authors' elaboration

Unclear scope for mobile health products and services. It was highlighted that harmonising the reimbursement of digital health services at a European level is not feasible nor relevant, given the number of coexisting reimbursement models and considering that this issue falls within the competences of the Member States. On the other hand, the European Commission could focus on the scope of services and the value of the outcomes.

⁴² <https://alliedforstartups.org/wp-content/uploads/2020/09/Telemedicine-report-2020.pdf>

According to many stakeholders involved in the consultation, one of the main gaps met so far, despite various attempts, is the clear definition of mobile health, since there is still a grey zone around the definition of mobile health and well-being apps. Indeed, it is quite challenging to define such a large field in order to classify every application, given that there is no specific legislation, specific basis set in the clinical guidelines for well-being apps, and that is unclear to what extent the processing of data in well-being apps is to be considered as health data processing under the GDPR. One important point that must be considered is the context of use (whether the patient on his own or as part of a treatment with additional requirements for the healthcare professional). Since reimbursement laws are still providing a narrow definition of mHealth, many stressed the evolution of eHealth, with mHealth becoming much broader as technology advanced. However, some stakeholders do not consider the term "mHealth" helpful for regulatory purposes, with a focus made on mobile devices and apps. Some medical technologies promoting people's and patient's mobility might not be comprised in the general scope for mHealth (e.g. technologies allowing patients remote treatments even though there is no mobile communication per se or implanted cardiac devices that are remotely monitored).

Some European initiatives⁴³ are working on defining the scope of such apps (including health and wellness). It has been operationalised by looking both at the origin of the service (e.g. platforms) and the area they apply to (e.g. physical, mental, social health). Since both medical device and non-medical device apps can be used in healthcare, a standard framework has for instance been adopted to understand the context in which the apps are intended to be used, as to better categorize them. Providing a shared view about mHealth, narrow or broad, would support the reimbursement of such technologies, since the driver rather revolves around what the technology is providing to enable the patient.

Complexity, redundancy and increasing regulatory requirements. Some barriers to digital health certification were caused by the lack of European legislation around liability and reimbursement issues and a complex market approval. Demonstrating outcomes is required in order to establish eHealth quality and efficacy, but some stakeholders are not satisfied with the sensitivity, validity, and reliability of existing outcome measures. There is a lack of understanding of the standards used in the design, production and implementation of software and hardware that should be used in remote monitoring systems (DiazSkeete et al., 2020). Regulation (EU) 2017/745⁴⁴ is the standard for the creation, oversight and processes used by manufacturers of medical devices within the European Union: the software used to run the device and process the data collected by the device is also considered as a medical device, but the standard also differentiates between "Wellness Devices" and "Medical Devices", where this last category undergoes a rigorous quality and risk assessment used for clinical, therapeutic or medical purposes. It has been highlighted by the consultation that HTA stakeholders are sometimes struggling to avoid redundancy in certification. There is a need to reduce the complexity and the length of such certification processes for all stakeholders. However, industry stakeholders highlighted during the consultation that rules should not be implemented on top of national specific requirements for certification/reimbursement, as not to put additional burdens that might add costs, effort and time for market access.

The position of the EU not to have a role yet in the assessment of mobile health which is not medical devices has also led to "soft" regulation (e.g. code of conducts and guidelines). It has been underlined that the organic and dynamic model of mobile applications development, constantly changing through regular updates, makes it difficult for a single body to keep up with

⁴³ <https://www.nen.nl/en/health-and-wellness-apps>

⁴⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745>

mobile health evaluation and certification, even if the MDR contains dedicated rules for updates to medical technologies and digital solutions. According to European stakeholders, mobile health applications are not very different from web-based health applications in terms of policy, and by classifying software as class IIa (cf. Rule11), there is a risk of delaying the introduction of innovative solutions.

Box 11. German Digital Healthcare Act⁴⁵

On December 19, 2019, the Act to Improve Healthcare Through Digitalisation and Innovation (Digital Healthcare Act) entered into force in Germany. It defines digital healthcare applications as "medical products with a low risk class whose essential function is mainly based on digital technologies, and which are intended to support the detection, treatment, alleviation, or compensation of injuries or disabilities." Insured persons have the legal right to claim for reimbursement for a mHealth app if it fulfills the two following conditions: (a) the app is included in the register of digital healthcare apps kept by the German Federal Institute for Drugs and Medical Devices (BfArM), (b) the app has been prescribed by a doctor or psychotherapist or has been used with permission of the statutory health insurance.

In order to be registered in the BfArM database as a reimbursed digital healthcare application, manufacturer should apply and provide evidence (a) of the safety, functionality, and quality of the app, (b) that their product fulfills data protection and data security requirements, and (c) that the app has a positive effect on care. Positive effects are either medical benefits for the patient or a patient-relevant structural or procedural improvement of care. If a manufacturer cannot yet prove a positive effect, the app may be preliminarily included in the register for up to 12 months. The manufacturer must submit a scientific evaluation from an independent third-party institution that discusses the positive effects and the required evidence must be submitted during the 12-month period. The trial period may be extended for another 12 months if the submitted evidence is not yet sufficient but the trial results indicate a strong likelihood that proof will be possible. A new application for inclusion in the register is possible only if new evidence is presented. Manufacturers negotiate the reimbursement to receive directly with the Central Federal Association of Health Insurance Funds.

Source: Authors' elaboration

Requirements differ vastly between countries and software products are no longer exempt from regulatory compliance (Hollmark et al., 2015). In France, the funding of telemedicine projects, and of eHealth projects in general, is characterized by a very controlling approach, centred around healthcare institutions resulting in rigidity and lack of transparency. The administrative burden holding back telemedicine in France must be relieved to give rise to local, non-hospital-dependent eHealth projects (Bouvet et al., 2015). This ties into the complexity of introducing digital healthcare. Any introduction of a new solution or modification of a care pathway to integrate a digital tool must first be analysed by a set of stakeholders (scientists, health professionals, insurers, etc.) often operating at different levels (national, local, etc.) but whose assessment of validity, value, safety, cost, etc. is necessary for its adoption.

Lack of data availability in a cross-border context. The lack of data availability is particularly observed in eHealth technology reimbursement due to the need for structured interoperability of eHealth services in a cross-border context, even if the action is supported by the development of the European National Contact Points (NCPeH) and MyHealth@EU (with the first two services promoted being ePrescription and Patient Summaries allowing access to this data in the 25 Member States to be deployed by 2025).

⁴⁵ <https://www.bundesgesundheitsministerium.de/digital-healthcare-act.html>

At Member State level alone, data accessibility is an issue. Not all citizens of the Member States have easy access to their health data and only a few countries allow patients to request the deletion of their EHR. Most Member States have set up competent authorities to facilitate the semantic and technical interoperability of their health tools, but only about half publish guidelines, maintain archives of the terminologies used, or propose correspondences with international standards. However, the translation of these standards is the main service offered by these authorities, but almost two-thirds of the countries add national extensions.

Considerable legal obstacles exist in a cross-border context when it comes to the use and exchange of electronic health applications (including e-prescriptions). For instance, the Dutch eHealth strategy was scaled down to establish a regional patient information exchange system, i.e. a dataset of essential health information, accessible for GPs, pharmacists and hospital-based medical specialists only. Central to this exchange system is the patient's explicit consent for exchanging patient information among regional health providers (opting in). Given the limited number of voluntary opting ins (5 million patients in 2014), the exchange of information remained modest with no upscale and cross-border use, therefore tempering the underlying objective of stimulating patients' self-management and movement across borders. (den Exter et al., 2015).

In a more general way, an improvement can be done on data availability to support evidence: as an example, the Estonian nationwide second-generation e-prescription should have had a more rigorous evaluation process during the implementation stage: the service has high usability and user satisfaction, but little empirical evidence is available to support the realisation of benefits (Parv et al., 2014).

Lack of trust from the users. Public European organisations' stakeholders emphasised the difficulty to find a practical way to harmonise reimbursement systems across borders, considering the implications for trust issues (e.g. what would it take for an individual to trust a health app from another country or people reluctant to share data cross-border). eHealth experts stressed the fact that although providing certification or endorsing a specific app to use for certain medical conditions would enhance clinicians' trust over digital services, they often need more than a self-certification from services providers, as to provide evidence of what is certified. It should be noted that articles 42 and 43 of the GDPR enable having a data protection seal or mark, for the purpose of demonstrating compliance with the GDPR, in order to add a level of trust, with, as a result, a confidence from the healthcare providers as well as individuals on the benefits brought to the patients.

Among the sources of barriers impacting the adoption of eHealth in common practices are: the lack of awareness about remote monitoring, the angst about the responsibility for the data generated, the design of systems, the regulatory standards, and the increasing demand on services, education, and patient empowerment (DiazSkeete et al., 2020).

Costs and benefits

Below is presented the synthesis of the perceived costs and benefits for the drivers and obstacles identified within this research area, through the impacts of harmonising the rules or not.

Table 3. Approval, certification, authorisation and reimbursement drivers

Drivers	Quality labelling	Common assessment practices	Innovative access pathways	Frameworks, assessment guidelines and code of conducts	Data evidence availability to support decision-making in cross-border care	Existing EU governance on assessment issues
Impact	+++	++	+++	++	+++	+
	--	-	---	-	--	-

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits.

Source: Authors' elaboration

Table 4. Approval, certification, authorisation and reimbursement obstacles

Obstacles	National fragmentation of health systems, financing and reimbursement models	Unclear scope for mobile health products and services	Complexity, redundancy and increasing regulatory requirements	Lack of data availability in a cross-border context	Lack of trust from the users
Impact	---	-	--	---	---

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits.

Source: Authors' elaboration

The national institutions' stakeholders interviewed clearly see the usefulness for the success of cross-border telehealth to clarify whether the Directive 2011/24/EU applies to healthcare, medicinal products and medical devices and the pathways that could be used.

It has been highlighted the role of frameworks and standardisation to overcome the current fragmentation. Although outside the EU's competence, an alignment of assessment and reimbursement systems in a single market logic would be even more important for smaller app developers, providing them a better ability to scale. Fair models with innovative pathways could support developing SMEs' opportunities and to reduce the difficulties they face when entering the industry, with harmonised requirements resulting in fewer customisation efforts. Besides, this would lead to better offerings and lower costs of digital health solutions to include private bodies, considering their added value in the process. It has also been highlighted the importance for the certifications to be electronic, mainly for transparency and safety reasons (which is an even more important point for non-EU vendors and producers, with a need for follow-up, verifiable credentials and claims).

A labelling would greatly help with transnational access to markets, and several stakeholders stressed that a certification for mobile apps will be required, in order to ensure confidence among healthcare professionals as well as to establish functional reimbursement mechanisms. A risk-

based approach led through the European regulatory framework with a case-by-case look could bring more clarity for eHealth stakeholders on the mobile apps market.

The fragmentation can lead to several issues: a lack of financial compensation resulting in the solutions not being adopted and used across EU countries, a lack of common digital health classification among European Member States, a lack of similar access pathways dedicated to digital health and a lack of harmonisation between countries on evidence requirements. Market access may depend on requirements, other than regulatory requirements, that are country-specific and hence vary from country to country, requiring costly customised approaches. Apart from funding on an experimental basis, administrative barriers in long-term funding hinder a sustainable development of eHealth innovations.

Although regulatory steps are needed for the mHealth market, a difficulty regarding compliance is mainly applicable to medical devices, where regulatory requirements are not only increasing the cost, but also the need for testing/evidence and collaboration between different actors.

2.2.3 Interoperability

Drivers

European EHR Exchange Format, documentation standards and minimum datasets. It has been highlighted through the consultation that the European EHR exchange format (EHRxF) can have a significant downstream effect, only if it is adopted. Industry representatives stressed the increasingly national healthcare systems requirements on developers to deliver data along certain specifications, with a serious risk of fragmentation. In this regard, the further development of the EHR Exchange Format recommendation, although its take-up seems to have slowed down, could cover specifications on data from devices and services, with a coordinating role to avoid multiple national recommendations or strategies and fully accomplish the potential of data and AI.

For a digitalization approach to be a success, existing practices in health care must be rationalized, simplified, and redesigned, since it must be thought-out to a different logic than the paper-based system (Pohlmann et al., 2020). eHealth experts highlighted the main principle for a minimal viable patient summary as not harming the patient and stated that some European projects (such as epSOS project) already worked on a minimum data set to be included in a patient summary with a cross-border care context, extended with more information into the International Patient Summary (IPS). It has been pointed out the need to start with the semantics rather than the technical interoperability, focusing on "transcoding" rather than "translation" as considering the potential impacts of translation errors. The term "interoperability" needs to be carefully defined to be meaningful: local, regional and national health authorities need to define the way data must be received. For instance, the MedTech industry focuses on the interoperability between medical devices and health IT systems and health IT systems between them.

eHealth Network. By establishing a European network of national eHealth authorities (art.14(3) of Directive 2011/24/EU), the Commission is facilitating cooperation and exchange of information. The eHealth Network participates in establishing a set of recommendations regarding interoperability. These guidelines are non-binding and addressed to the Member States of the European Union. The following elements were especially established and shared with the Member States by the eHealth network:

EHR: recommendations seeking to facilitate cross-border interoperability of electronic health records (EHRs) in the EU by supporting Members States in their efforts to ensure that citizens can securely access and exchange their health data wherever they are in the EU. The objective

is to help citizens quickly access and share their health data with healthcare professionals when consulting a specialist or receiving emergency treatment in another EU country. It promotes a step-by-step approach to create interoperability of electronic health records at an EU level, through the brand MyHealth@EU, a mission of the eHDSI (eHealth Digital Service Infrastructure), building on the European domains of Patient Summary and ePrescription information⁴⁶ (datasets, recognition and delivery of prescriptions, roadmap to extend EHR interoperability to 3 new domains: (1) laboratory results, (2) medical imaging and reports and (3) hospital discharge reports). The 2019 European Electronic Health Record Exchange Format Recommendation⁴⁷ issued technical and organisational recommendations in order to support the implementation of HER, including the use of the Refined Interoperability Standards, the five baseline data that need to be made available and the preferred organisation of national networks. This recommendation was supported by the X-eHealth⁴⁸ project, launched on September 2020, in which four of the eight workpackages focus on technical-functional activities.

Patient registries: methodological guidelines for efficient and rational governance of patient registries, written by the PARENT Team (PA^Tient RE^Gistries iNiTiative), created to provide practical advice for the set-up and management of patient registries, as well as to enable secondary use of data for public health policy and research.

Applications interoperability: a list of 10 communications and documents, of which a set of interoperability guidelines for approved contact tracing mobile applications in the EU and for cross-border transmission chains between approved mobile applications, but also a work on semantic coding and vaccination certificates. Among those actions, in November 2018 the eHealth Network (eHN) endorsed the work of the Working Group on Common Semantic Strategy (CSS) created in the eHAction joint action to come up with a solid proposal for a five-year strategy to be discussed as a draft in May/June 2019 and approved in November 2019.

Box 12. Patient Summary implementation within Member states

According to a recent survey realized by the eHDSI Community (National Patient Summary Survey 2020⁴⁹) on patient summary implementation, the implementation is limited but in progress: out of the 12 responding Member States, only 5 completed the implementation of a patient summary at a national level and the other 7 Member States are still in the process of implementing their patient summary. Interoperability standards are well shared: almost all MS used the same interoperability standards, namely HL7 CDA and/or HL7 FHIR, HIE profiles and OpenEHR. However, the data scope often matches only partially with a provision of services in a cross-border context.

Source: Authors' elaboration

International and European interoperability standards. Through the development of multiple databases, software and the growing need for interoperability between these tools over the years, several health-data formats and nomenclatures became shared references: EMR, EPR, HL7, IHE, etc. (Aceto et al. 2018).

⁴⁶

[https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en#:~:text=ePrescription%20\(and%20eDispensation\)%20allows%20EU,to%20their%20country%20of%20travel](https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en#:~:text=ePrescription%20(and%20eDispensation)%20allows%20EU,to%20their%20country%20of%20travel)

⁴⁷ <https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format>

⁴⁸ <https://www.x-ehealth.eu/about/>

⁴⁹

https://ec.europa.eu/cefdigital/wiki/display/EHMSEG/04_Other+relevant+national+characteristics+of+Patient+Summaries

Health Level Seven International (HL7) is a not-for-profit ANSI-accredited standard developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing and retrieval of electronic health information⁵⁰. It supports clinical practice, management, delivery and evaluation of health services. The HL7 mHealth Working Group creates and promotes health information technology standards and frameworks for mobile health (Chronaki et al., 2016). The HL7 offers only four certifications for individuals to prove their understanding of HL7 standards.

The new European Interoperability Framework (EIF) defines interoperability, within the context of European public service delivery, as “the ability of organizations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organizations, through the business processes they support, by means of the exchange of data between their ICT systems”⁵¹. It offers basic interoperability guidelines in the form of common principles, models and recommendations for the delivery of European public services. It encourages public administrations to design and deliver services that are providing services and data preferably via digital channels, accessible for all citizens in the EU, enabling reuse, participation, access and transparency, as a standard approach for the design and operation of European public services.

Integrating the Healthcare Enterprise (IHE) is an initiative led by healthcare professionals and industry representatives to improve the way computer systems share information in healthcare. Integration Profiles describe clinical information management use cases and specify how to use existing standards (HL7, FHIR, IETF, DICOM, OASIS, ISO, etc.) and to address them both for equipment vendors (implementation guides) and healthcare providers (guidance for integration requirements in purchasing). In 2015, the European Commission published the Commission Decision 2015/1302, identifying 27 HIE profiles to be listed in public procurement.⁵²

The eStandards initiative (2015-2017) has been funded by the European Commission to develop a roadmap for the construction and adoption of eHealth standards and specifications. Stakeholders in Europe and worldwide worked together to build a consensus on the steps towards the interoperability of health data standards, aiming at accelerating knowledge sharing and promoting the rapid and widespread adoption of standards.

FAIRness for FHIR (FHIR4FAIR⁵³) project has the objective to connect the FHIR standard to the FAIR data principles (Findable, Accessible, Interoperable and Reusable) as well as to facilitate the collaboration between both communities. Using automation and AI for these types of projects would help the European life sciences and healthcare sectors by improving data quality

European Interoperability Initiatives. Since the Directive 2011/24/EU, many projects dealing with interoperability were launched at a European level. Among them are some relevant initiatives listed below.

KONFIDO⁵⁴ was a secure and trusted paradigm for interoperable eHealth services. It intends to provide a scalable approach for secure inner and cross-border exchange, storage and handling of healthcare data. In order to address the challenges of secure storage, exchanges, security

⁵⁰ <https://www.hl7.org/>

⁵¹ https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF

⁵² https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_199_R_0011

⁵³ <https://confluence.hl7.org/pages/viewpage.action?pageId=91991234>

⁵⁴ <https://konfido-project.eu/>

and personal data control, KONFIDO takes on an approach by targeting all architectural layers of an IT infrastructure, such as storage, dissemination, processing and presentation.

epSOS project⁵⁵, predecessor of eHDSI/MyHealth@EU, ran for six years (2008-2014) and set out to develop, pilot and evaluate cross-border eHealth services, and to formulate recommendations for future work, with a focus on safe, secure and high-quality services for exchange of patient summary data and ePrescriptions between European countries. The epSOS architecture is implemented as a set of interacting National Contact Points (NCPs) built on top of Web technologies (SOAP). The model of the epSOS platform can be viewed as a federation of services connected with service interfaces defined by specified contracts.

ISA² Programme⁵⁶ supports the development of digital solutions that enable public administrations, businesses and citizens in Europe to benefit from interoperable cross-border and cross-sector public services. Under 54 actions, organized in 9 workpackages, the programme develops interoperability solutions generally available for free.

OpenNCP framework offers a set of interoperability services to enable national and regional eHealth platforms to set up cross-border health information networks. The framework is available as open source software and has been adopted in 12 Member States (Croatia, Hungary, Malta, Estonia, Luxembourg, Slovenia, Finland, Portugal, Italy, Sweden, Spain, Greece). OpenNCP provides a verified framework to build “National gateways” to foster an eHealth ecosystem across Europe (Fonseca et al. 2015).

eHealth ERA project (Towards the Establishment of a European Research Area) contributes towards greater transparency across Member States and other participating countries on eHealth strategies as well as innovation-oriented research and technology development (RTD) initiatives, including the coordination of Member States’ eHealth strategy formulation and implementation.

The Commission financially supports the work of 3 European standardisation organisation: ETSI (European Telecommunications Standards Institute), CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization).

Inclusion of interoperability in eHealth quality label. In order to encourage software publishers to use listed frameworks, some Member States have already included interoperability guidelines or standards within their certification or authorisation process for eHealth services provided cross-border. A European eHealth labelling could include as a criterion a cross-border interoperability between digital health services, systems and EHR. To that end, it has been suggested that specific bodies could provide such interoperability label to the manufacturers and contribute to an overall quality label, in cooperation with HTA and notified bodies, with the perspective to incentivise the exchange of information between healthcare providers of digital health services and products.

The Nivel study commissioned by the Commission (2020) revealed that in a context of data sharing, some countries provide the opportunity to transmit health care provider-controlled data held in an EHR to a record controlled by a patient, such as a PHR or other system by which a patient can directly access data held by HCPs (more details are available in the section “Use of health data” of this report, under chapter 5). The other way of transferring health data, i.e. from an application to patient’s EHR, can be illustrated by the setting up of a personal digital health space under French Health law project “Ma santé 2022” including a set of health applications

⁵⁵ <https://ec.europa.eu/digital-single-market/en/news/cross-border-health-project-epsos-what-has-it-achieved>

⁵⁶ https://ec.europa.eu/isa2/home_en

and services. To this end, applications must be compatible and certified with a compatibility label.

eHDSI/MyHealth@EU. The eHealth Digital Service Infrastructure is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF). It sets up the basic services needed for the exchange of ePrescription and EHR at a cross-border level, aiming at integrating the assets of epSOS, STORK, EXPAND and eSENS in a global solution. As highlighted during the consultation, such an organisation could provide guidance not only through implementation guides for APIs but also through key aspects on which some national stakeholders expect an action: (i) **unique identification** through a pan-European identification system to enable a secure European patient and healthcare provider identification, along with the identification of their relation, (ii) **technical and semantic interoperability** towards a common understanding of medical information and a reduction in medical and prescription errors, as well as (iii) **security for the most sensitive data** through standards approval.

For now, an ePrescription and Patient summary exchange are possible through MyHealth@EU/eHDSI between Croatia, Estonia, Finland and Portugal, Malta, Luxemburg, Czechia. Finland is a relevant example within this domain, considering its Electronic Prescription Act, where: prescriptions are stored in National Prescription centers, pharmacists can access the prescription only with the patient approval and prescriptors must inform the patient and ask for his consent (data is preserved for 30 months).

The eHDSI structure can also support the exchange of patient summaries. By 2025, both services (cross-border ePrescription and exchange of EHR) should be implemented in 25 Member States, i.e. all except Bulgaria and Denmark. For now, EHR exchanges are becoming available in Croatia, Czech Republic, Luxembourg, Malta and Portugal, with a gradually approach, i.e. data sharing is one-way accessible (see Annex 7.7).

Public funding. The referencing of specific tools is a common practice in public procurements, which could include mandatory standards and specifications supporting cross-border interoperability. Over 76% of the EU budget is handled through partnerships with national and regional bodies through a management divided in five main funds, with other funds being handled directly by the EU. To support eHealth programs, Member States can benefit from several European funds such as EU4Health⁵⁷, the Digital European Programme⁵⁸, the European Regional Development Fund (ERDF), the European Social Fund (ESF)⁵⁹, the Cohesion Fund⁶⁰ or the Recovery and Resilience Facility (RRF)⁶¹. According to the specific regulated aims of each fund, some conditions need to be met to benefit from funding. For instance, the ERDF specifies four key areas of priorities: (i) Innovation and research, (ii) the digital agenda, (iii) support for small and medium-sized enterprises (SMEs) and (iv) the low-carbon economy. It is to be noted that the ERDF, the ESF and the RRFs' plans are open to each of the 27 Member States, whereas the Cohesion Fund is open only to a set of Member States for a six-year duration.

In addition, eHealth Network Guidelines on an interoperable eco-system for digital health and investment programmes for a new/updated generation of digital infrastructure in Europe⁶² states that public funding is made available by the EU Member States and the European Commission to be used for updating existing or establishing new digital health infrastructures, must be used

⁵⁷ [EU4Health | European Commission \(europa.eu\)](https://ec.europa.eu/health/eu4health_en)

⁵⁸ [Digital Europe Programme | European Commission \(europa.eu\)](https://ec.europa.eu/digital-single-market/en/digital-europe-programme)

⁵⁹ <https://ec.europa.eu/esf/main.jsp?catId=35&langId=en>

⁶⁰ https://ec.europa.eu/regional_policy/en/funding/cohesion-fund/

⁶¹ https://ec.europa.eu/info/strategy/recovery-plan-europe_en

⁶² https://ec.europa.eu/health/sites/default/files/ehealth/docs/ev_20190611_co922_en.pdf

to support the establishment of a European interoperable eco-system for digital health, while taking into account the national interoperability strategies.

European eHealth experts highlighted during the consultation that such conditionalities for EU funds (ERDF, RRF, etc.) and state aid could be aimed at financing digital health, for instance under ex-ante conditionality to comply with specific standards and specifications ensuring interoperability between m-health and EHRs.

Obstacles

Legal barriers for cross-border scale-up. During the consultation, one eHealth expert highlighted that Directive 2011/24/EU is becoming quite outdated, based either on organisation-to-organisation or physician-to-physician interoperability models, which has hampered the acceleration of patient-centred interoperability. It has been reported that even though some laws do allow for patient mediation, a more careful in-depth analysis is needed to prevent misinterpretation and to push the stakeholders into the will of a change.

The effective scale-up of applications at an international level remains difficult for the industry, primarily due to the diversity of legal frameworks and the lack of mutual recognitions towards the dimension of a digital single market. The concept of evaluation remains unclear from one Member State to another, with a subsequent need to "start every process from the beginning" while some countries implement their own national processes. An on-going work is currently carried out on ISO standards, potentially included in quality and liability mobile health assessment (cybersecurity, interoperability, data protection and reliability), however they are still not effectively used for certification.

Lack of alignment on interoperability. Large-scale EU projects which focused on interoperability (e.g. epSOS, Open NCP) brought provisional legal agreements (Martins et al., 2014) in some countries (notably patient summaries and e-prescriptions within Spain and Denmark) along with pilot cross-border services. However, their scope remains limited, with a slow pace of development. The current framework relies on technological, legal and procedural interoperability based on agreements between individual member states (Kautsch et al., 2017). Key barriers were also identified in the development of the KONFIDO project, among them: the lack of alignment of the Member States with the eIDAS Regulation and the JASeHN agreement, the lack of EHR systems among Member States, the existence of different and complex consent mechanisms, or the different implementations of EU regulations (Nalin et al., 2019). Especially, a lack of integration/interoperability is observed by the consultation stakeholders between other eHealth services and electronic health records. In Sweden, none of the 21 regions and 219 municipalities are fully able to share all their data with other Swedish regions, even though a national Swedish patient summary has been set up. As a result, the Belgian eHealth platform has developed an interoperability testing workbench for developers to uniformly test their applications. This test bench has helped to refine the medical software market and facilitate visibility and transparency for all stakeholders. For digital health solutions to be deployed, standards are needed to support the secure and reliable exchange of health data between the many IT solutions used by health professionals and the many IT solutions used by patients. Without these standards, each exchange involves customised calibrations that are very costly.

According to eHealth experts, one of the main barriers identified is the non-binding nature of the European guidelines, since Member States can either follow the standards or not on a voluntary basis: despite its important work on interoperability standards, the recommendations outcome by the eHealth network remain not binding. Furthermore, the interoperability implementation has mainly been carried out organisation to organisation rather than in a patient-centred way and only a few tools are truly supranational. However, healthcare pathways are

mainly local or regional, with specific requirements on the interoperability needs of digital health services and products. Thus, interoperability practices are not easily translated to European interoperability requirements.

As highlighted in the Green paper on mobile health from the European Commission⁶³, the slow uptake of international interoperability standards is even more problematic for the app market as it is dominated by SMEs and individuals (i.e. app developers). This poses the risk of a fragmentation of standards (a summary of the main medical standards is available in Annex 7.8). In Germany, mHealth programmes are split into three groups: accessing/providing health services, accessing/providing health information and collecting health information. However, isolated solutions are prevailing, with challenges on interoperability not being dealt with. An analysis of a WHO survey showed that mHealth is "characterised by small-scale pilot projects that address single issues in information sharing and access". The literature review suggests that mHealth projects lack a complex design targeted at point solutions (Cwiklicki et al., 2020).

Box 13. Article 14 of the Directive 2011/24/EU

Interoperability in the USA

Many researchers highlighted as obstacles for interoperability the lack of clear political regulations and political incentive structures as well as unsatisfied requirements of regulatory authorities (Kouroubali et al., 2019). Several weaknesses have been stressed in the plurality of actors and electronic systems concerned (Pohlmann et al., 2020). Most eHealth experts agree that reaching interoperability standards is a prerequisite for the successful implementation of a PHR, nevertheless, due to such diversity, meaningful actions towards interoperability are still scarce. When analysing the implementation of telehealth within health centres in the USA, one of the main reasons cited for not using telehealth was the lack of interoperability between EHR systems (Lin et al., 2018).

Patient engagement is hindered by the lack of consistent and sharable consent policies. Furthermore, provider adoption is limited by a lack of consistent quality of data and integration into the natural workflow, which impacts user benefits and outcome improvements (Donahue et al., 2018).

Source: Authors' elaboration

Costs and benefits

Below is presented the synthesis of the perceived costs and benefits for the drivers and obstacles identified within this research area, through the impacts of harmonising the rules or not.

Table 5. Interoperability drivers

Drivers	eHealth Network	International and European interoperability standards	European Interoperability Initiatives	European EHR Exchange Format, documentation standards and	Inclusion of interoperability in eHealth quality label	eHDSI/ MyHealth@EU	Public funding
Impact	++	++	+	++	+++	++	+++
	--	--	--	---	-	-	-

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

⁶³ https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5147

Source: Authors' elaboration

Table 6. Interoperability obstacles

Obstacles	Legal barriers for cross-border scale-up	Lack of alignment on interoperability
Impact	---	--

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

Source: Authors' elaboration

The economic challenges seems to be the main source of the lack of interoperability in the healthcare sector, as well as the uncertainty of known individual costs achieving interoperability, as regulatory requirements and interoperability policies differs and differ per organisation , despite the matter being discussed in the literature for decades. Despite the wider adoption of interoperability standards in the past few years, there is too much variation in the standards themselves and how those standards are deployed. Thus, the costs of an interface project that needs to move data from one healthcare software platform to another may face significant fees from the source and destination system vendors.

However, it has been stated in the consultation that the costs related to the lack of interoperability are huge: especially, the absence of standards for labelling or certification mandating interoperability between eHealth solutions (software for pathologists, personal health data spaces or electronic health records),and devices seriously hinders innovation and economies of scale. Besides, this prevents digital Health investments from being correctly guided and limits the scalability of such solutions. Moreover, the setting and agreement on open interfaces would significantly simplify and accelerate the process of digital transformation and at the same time reduce the costs of digital-induced change. It implies better care coordination and patient experiences through less administrative tasks related to document and data management.

Besides, interoperability improves patient care through efficient exchanges of information. A meaningful use of EHR's programs can bring down the costs and improve Electronic Record information traceability, avoiding unsecure paper processes for collection of information. Interoperability can help enhance the privacy and security of patient data by requiring organizations to fully assess their organisation. Lastly, it supports faster decision with more accurate collection and interpretation of public health data when IT systems are able to interact.

Given the work already carried out and considered in the baseline scenario, in terms of benefits for harmonising interoperability and avoid those obstacles, we considered a decrease of 5% of costs for the patient journey if such an harmonisation is provided, with respect to the baseline scenario with no harmonisation, then possibly reaching 3.7 billion euros in total for patient journeys costs.

The consultation showed that an interoperability label would have an important positive impact to inform digital health stakeholders. Moreover, it could facilitate international market access for industry solutions by setting up a scale on requirements. eHealth experts underlined that the OpenEHR and the HL7 FHIR standards are at a maturity point where smaller companies can innovate in order to bring down the costs related to healthcare, while also increasing the efficiency gains in the interaction between different healthcare providers.

2.2.4 Data protection and liability

Drivers

Secure access to ePrescription and EHR. Secure deployment of ePrescription and EHR were a top priority for the European eHealth action plan, since they are considered to enhance the safety of data sharing and the compatibility of prescription in cross-border care, in a more understandable and trustworthy way. At a national scale, different approaches were observed, raising the issue of flexibility in the MS implementations: regional or national ePrescription⁶⁴ systems, mandatory or voluntary, in a centralised or decentralised way. On a practical point of view for the EU, as stated in Directive 2012/52/EU, cross-border prescriptions should include the following personal information: patient's surname, first name and date of birth; prescription's date of issue; information on the prescribing professional (surname, first name, professional qualification, direct contact information, work address and signature); information on the medicine (name of the active substance, pharmaceutical form, quantity, strength and dosage regimen). Six main types of data that Member State should include in their national implementations were defined by Recommendation on EHR exchange format: patient Summary (important health related aspects such as allergies, current medication, previous illness, surgeries, etc.), ePrescription/eDispensation, laboratory results, medical imaging, reports and hospital discharge reports.

In order to provide the secure access needed, a work on cross-border eHealth authentication has already been carried out resulting from the Directive 2011/24/EU (Katehakis et al., 2016). The further regulation should ensure that access and portability of patients' digital health records is compulsory in all the cases where a digital health service is provided (e.g. the doctor should be able to access the patients' EHR during an act of telemedicine; or the information should be transmitted to the healthcare professional and to the EHR of the patient in the case of tele-monitoring by a foreign healthcare professional). National digital health platform stakeholders stressed during the consultation that card-to-card authentication schemes, which are widely used in national healthcare systems, are still not appropriate for cross-border care services, lacking common identification methods.

Box 14. EHR authentication

In 2017, a survey was launched in each Member State for report of the JAseHN project (including Great Britain and with no answer from Poland). The results showed that authentication for accessing EHRs from a patient point of view was highly disparate, with 7 different categories of authentication and the following assessment:

- 9 MS use a national ID (such as social security number);
- 7 MS has an electronic signature or digital certificate;
- 5 MS could not identify their authentication scheme to any of the suggested schemes.

Source: Authors' elaboration

The ISO offers international technological security standards as well as certifications, to which it is relevant to comply for eHealth services (especially ISO/IEC 27000-Series and ISO 22600). The ISO/IEC 27001 offers requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving formalised information security management models as well as their alignment with the organisation's strategic goals.

⁶⁴ https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en

GDPR implementation. The General Data Protection Regulation 2016/679 (GDPR) sets forth a number of core principles for the collection and processing of personal data, such as lawfulness and data minimisation, and allowing the processing of sensitive data, including health data (Article 9) only in specific cases. The GDPR states that processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected (Article 5(1)(b) and recital 50). Consistent with the legal framework provided by the GDPR, informed consent provisions can play a key role in liability issues.

However, from a legal perspective, European industry representatives highlighted that the GDPR might not be fully or consistently applied among the MS, with a need to review the different GDPR implementations. Furthermore, it is considered not to encompass the specificities of digital health: definition of health data in GDPR is broad, but is not sufficiently detailed / specific on what exact categories of data would be included within that scope, only referring to "personal data which relates to the physical or mental health of an individual", without including well-being or lifestyle data generated with mHealth applications (den Exter, 2017). Health professionals explained that the unclear definition of "health data" led to a global lack of understanding around the processing, sharing and relevance of data generated by mobile applications, which should be dealt with in order to provide cross-border eHealth.

Box 15. An example in Pomerania: the Telepom project⁶⁵

Launched in 2001, the Telepom project connects 18 German and 15 Polish clinics through videoconferencing and data transfer. It enables rural hospitals to consult experts in urban hospitals and provide specialised services. In depopulated areas affected by demographic changes, this telemedicine network ensures that medical specialists can follow enough people without affecting the quality of the services provided. It now covers telemedical services in several fields.

A key success factor of the project was to meet different regulations regarding security of personal data (i.e. national, regional) as well as to ensure data anonymisation. An organisation was built to develop an in-depth understanding of the health systems on either side of the border and discuss with the state representative (Mecklenburg Vorpommern) for data protection. Other key factors were identified, such as translators for videoconferencing or the inclusion of the different cultural perceptions when presenting the information.

Source: Authors' elaboration

Codes of conduct to complement the EU Medical Device Legal Framework. The EU Medical Device Legal Framework is currently the only health-related official regulation applying to mHealth apps. However, several mHealth apps don't fall under specific regulation, not being considered as medical devices (sometimes named "borderline apps"). The dynamic nature of mobile health applications complexifies the implementation of an efficient assessment. Especially, apps traceability is a major concern addressed by recent EU guidelines that offer general and specific questions, guiding stakeholders in the self-assessment of the credibility or the strength of the apps and their functionalities (Mantovani et al., 2017).

Therefore, risk assessment could be an option to assess mHealth apps and would imply to distinguish medical and non-medical apps, opening the doors to independent scientific advice on safety-related aspects. Several attention points are to be highlighted on digital health safety: Member States (France for instance) developed their own secured tool for medical messaging between healthcare professionals; besides, the use of instant messaging (IMapps) between HPs

⁶⁵ https://ec.europa.eu/regional_policy/fr/projects/poland/telepom-uses-ict-to-improve-medical-care-in-rural-areas-at-the-german-polish-border

and patients or peer-to-peer is constantly increasing (Morris et al., 2019) ; lastly, mHealth apps are currently available through generic marketplaces, among which, in a review of 70 mental health apps (Parker et al., 2019), it was noticed that only Google Play store distinguish 'higher risks' permissions, and that several mHealth apps do not comply with GDPR.

In order to stress out its potential, its main issues and its role in healthcare systems, a Green Paper⁶⁶ on mobile health has been issued in 2014 by the European Commission. The first versions of Code of Conduct for mHealth apps⁶⁷ were prepared against the background of the mHealth Green Paper consultation. A general perception has been that people often do not trust mHealth apps because of privacy concerns, which was confirmed during the consultation by patients representatives who also shared this view. As highlighted through the consultation, this code of conduct could be the first step for labelling mHealth applications, however, it is not in place yet, because no stakeholder has taken responsibility for managing the Code (as Code author) in accordance with Art. 40 and 41 GDPR.. Developers would declare their adherence to the Code by completing the privacy impact assessment and a self-declaration of compliance to the Monitoring Body. Once checked and approved by the monitoring body, the application would be identified in a centralised public register. If willing, the developer could undergo under a third-party audit and certification of compliance. However, it was also stressed that no EU code of conduct on data protection related to healthcare has been approved yet by the European Data Protection Board, not even at national level. Lastly, three codes of conduct approved by the EDPB⁶⁸ were mentioned by healthcare representatives.

It must be noted that the AIA proposed by the Commission in April 2021 provides the possibility to adopt codes of conduct, notably for low-risk AI systems which are not subject to mandatory certification requirements.

Patient mediation through transparency, right information and appropriate consent model. The adoption of services is mainly due to barriers to the adjustment of societal behaviours. Among these barriers, defiance, distrust or misunderstanding about security and liability matters are central. It was stated during the consultation that accountability and transparency are key elements to ensure trust, therefore one should find the means to constantly ensure transparency on security and liability issues towards digital health adoption. Whereas transparency is a main principle of Quality of Services, it is not yet widely implemented within regulation frameworks (Spagnuelo et al., 2017). Some properties were offered to qualify transparency such as openness, availability, auditability, verifiability, empowerment, usability and privacy.

The control of patients over data could be emphasised through GDPR in mHealth regulation: the data-subject could decide on the storage (e.g. EHR, device) and the sharing of data. This would eliminate any obligation for the patient to store his mHealth data on the servers of the manufacturer, and ensure the data cannot be processed in a country not covered by GDPR or limited to the EU/EEA and cannot be shared with third parties (e.g. employer, insurer) unless requested explicitly. It has been suggested during the consultation that European healthcare organisations could agree on paying liability fees to patients for any error made with their data. The BIGPICTURE project⁶⁹, led by RadBoud UMC, helped in the creation of the first European,

⁶⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0219&rid=5>

⁶⁷ <https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps#:~:text=%20Privacy%20Code%20of%20Conduct%20on%20mobile%20health%20industry%20stakeholders%20in%20order%20to...%20More%20>

⁶⁸ https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en

⁶⁹ <https://www.radboudumc.nl/nieuws/2021/nieuwe-europese-samenwerking-met-innovative-medicine-initiative-wil-grootste-pathologie-databa>

ethical and GDPR-compliant, quality-controlled platform, based on large data files and AI algorithms. National institutions stakeholders stressed that such projects will lead to a broad understanding of pathology data, will help connect healthcare sites at an international level and are an important first step towards initiating European data spaces.

Industry and HPs representatives agreed on the need for a better communication towards patients about the various benefits of sharing their health data, which would likely make them more willing to do it. Healthcare professional representatives explained that patients are often more inclined to share their health data for specific causes such as cancer, Covid-19, chronic or rare diseases. Furthermore, it has been stressed during the consultation that the user should always be asked about the information to be added to its summary in a cross-border context: it should not systematically appear in a patient summary if it represents a direct risk for the person (e.g. to avoid exposing an act considered illegal in the country of origin). These culture and national gaps shed light on the need for "third consent": data must be patient-controlled rather than a "free flow", and such patient mediation should be promoted through legislations.

Box 16. International Medical Informatics Association Code of Ethics

While several security and privacy standards have a general ethical basis, there are mainly focused on the technical development of health informatics products. The IMIA is an international health informatics organisation intended to promote healthcare innovation at an international level. IMIA released a Code of Ethics for Health Information Professionals and initiated a long-term project, the Global Protection of Personal Health Data, in order to identify the requirements for protecting personal health information within an international context.

Several ethical codes were released by organisations without being used by professionals (HIP). Therefore, it was offered to set up an international certification with a collaboration of WHO National Bodies with IMIA, on privacy and security aspects, both for the HIP and their organisation (Kluge et al., 2018).

Source: Authors' elaboration

Better regulation guidelines and Product Liability Directive. Keeping the pace of change and innovation should be done in a way which is consistent with other works being undertaken at an EU level, such as adherence to the Commission's Better regulation guidelines, which seek to provide a simple, clear, stable, and predictable regulatory regime for businesses, workers, and citizens. Furthermore, industry representatives believe that the Product Liability Directive ensures satisfactorily liability for defective MedTech products and contributes to a reasonable balance between protecting and ensuring fair competition.

Obstacles

Various, complex and highly demanding privacy frameworks. Apart from GDPR and Directive 2002/58/EU, some countries developed their own legal framework for digital health and are either still engaged in the process or struggling with a highly demanding system, sometimes going from incomplete legal frameworks to very strict ones. The review of interoperability and software security frameworks shows that there is not a full adherence to the targets set by international standards for information security due to difficulties to comply with the standards. Furthermore, with the rapid evolution of technology, cybersecurity frameworks can quickly become outdated (Natsiavas et al. 2018).

Italy started to implement a national EHR in 2012 but the legal framework is still highly incomplete and difficult to read (Bologna et al., 2016). Indeed, Act 221/2012 insists on informed consent and the role of healthcare professionals to explain clearly the EHR purposes, there are still no professional qualifications within this field. Moreover, minors' data protection is

completely missing in this act. Privacy rules result from a complex mix of Act 211/2012, Data Protection Code general principles and Data Protection Authority guidelines.

In Germany, personal data and privacy regulations (German Privacy Act, BDSG-New) are particularly highly demanding. Strict data protection laws in the area of health has been set out locally: "For example, the plan for the electronic health card envisioned that the patient could only inspect his medication data together with a doctor or pharmacist, or in an "environment that ensures that the patient's rights can be safely executed".

Box 17. Privacy frameworks in North America

In Canada, there is substantial variability across regulatory bodies in the scope, specificity and robustness of mHealth regulations, with Canada's regulatory framework lacking in two major domains: (1) specificity of existing regulations for mHealth and (2) regulatory clarity for what apps require regulation (Jogova et al., 2019).

The US and the EU differ notably in their regulation policies : while in the US the Office for Civil Rights enforces the Health Information Portability and Accountability Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information; in the EU the GDPR (General Data Protection Regulation, (EU) 2016/679) regulates since May 2018 the processing of personal data across the 27 Member States. In both continents and countries, conventional healthcare is highly regulated, and even though regulations exist, ICTs-based healthcare services are still generally perceived as under-regulated, raising questions about quality, safety, and data protection (Aceto et al., 2018).

Source: Authors' elaboration

Uncertainty around liability and safety rules. eHealth experts underlined the importance of liability when considering cross-border healthcare and emphasised that Europe should not follow the example of the US, where it is mainly associated with fear. The European Commission could have a role in setting the boundaries across Europe, since it is a relatively recent and major issue that countries have to deal with.

Liability and telehealth/telemedicine. Some concerns were raised during the consultation about responsibility and data access: it should be noted that some providers could be afraid of privacy concerns to the point that they are potentially depriving patients of the health benefits that they could get from such services, even if such benefits have been proven. In addition, harmonised standards are often used as a mean of achieving compliance with EU product safety laws, however the challenge for emerging technologies is that standards often cannot keep the pace with the speed of product change and innovation. Besides, from a healthcare professional point of view, digital health solutions must be fully integrated in the current daily practice workflow.

Liability and mHealth. Healthcare professionals' representatives valued two use cases in the consultation: (i) the patient looks for a service or downloads a health app on his own, (ii) a healthcare provider prescribes the use of an app. It was stated that the use and prescription of digital tools should only happen if there is a pre-existing relationship with the patient and under certain conditions to be defined (e.g. follow-up, monitoring, post-operation consultation). Apart from the provider accountability, questions were raised around the professionals' or the patient's responsibility and accountability. HP representatives highlighted the need to clarify the legislation regarding the prescription of non-medical apps (e.g. instant messaging, data transferring), explaining that clinicians are currently responsible for any prescription, even for non-certified services. It was stressed that the context should be considered: if a well-being app is used in a medical framework for diagnosis or monitoring, a prescription is needed. However, healthcare professionals generally face difficulties in recommending the best mobile health

application for their patients because they are not fully able to assess how they were developed and ask for their involvement in such process to enhance clinicians' trust.

Liability and AI. It was mentioned during the consultation an ongoing DG JUST study intended to support the Commission's Policy Development on Liability for Artificial Intelligence.

Lack of framework for patients' control over their health data beyond GDPR. Healthcare professional representatives emphasised that the GDPR is not sufficient to protect the use of data in the medical research field, since patient consent in medical research goes beyond simple GDPR consent, as the GDPR requires "explicit consent" of the data subject (Article 9). Besides, healthcare representatives stressed the need to embed the principles of the Taipei⁷⁰ and the Helsinki⁷¹ declarations on the management of personal data in medical research, to ensure control over health data processing. Industry representatives highlighted the differences between Member States approaches around the health data processing regulatory framework, stressing the national GDPR implementations which focus on the patient consent or turn towards public health interest. For the benefit of the digital health market, a legal clarity on compliance regulation surrounding the use of health data is needed.

Besides, a lack of technical means has been identified by industry representatives regarding data exchange and proper access to data in electronic format. European patients' representatives agreed on the complexity for many patients to access, use and amend their information: more clarity is needed about the rules and frameworks regulating control and access of health data in electronic format, especially on a cross-border level. In 2019, the European Patients Forum carried out a survey on patients' perspectives of EHRs, which showed both a need for a better collaboration between healthcare professionals and for a removal of technical barriers to data access. Potential keys would be the application of literacy-by-design and patient-friendly principles to improve adoption of digital health tools.

Furthermore, it was pointed out the lack of information on the value of data sharing, prior to consent, the difficulty for a patient to understand specific legislations on data, and the need for efficiency in the consent process. A crucial information-sharing role is held by clinicians, who often lack time to dedicate to this role. Therefore, a more professional way of communicating about data should ensure that information is provided in a "tailored" way, through the concept of research for the "public good" and the consideration of any potential ethical objections that patients may have on the secondary use of their data. Healthcare providers should be able to explain how and why the data is used, even including anonymous data, which is not covered by the GDPR (according to HP representatives, the default rule for sharing patient data for secondary purposes should be anonymisation). However, this need highlighted the difficulty for a doctor to have a correct overview of the secondary use of the data.

The future EHDS (European Health Data Space) aims to increase people's access to electronic health data, which raises concerns about the rules on data processing that will be used. The proposed Data Governance Act⁷² and associated data governance framework structuring the EHDS are expected to support patients with a balance between the right level of access and control over their data and the possibility to unlock it for the public good.

⁷⁰ [Declaration of Taipei – WMA – The World Medical Association](#)

⁷¹ [Declaration of Helsinki – WMA – The World Medical Association](#)

⁷² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>

Consent model granularity. eHealth experts stressed the importance of “re-consenting”, which covers the authorisation for reusability of patient data in other contexts. Industry representatives expressed that some technical issues have not yet been addressed regarding the granularity of consent, to find the balancing point for citizens when giving their consent. It encompasses a difficulty to identify the level of request to the user and to provide information to the patient at the right level, considering the many different perspectives among the populations. The best consent mechanism is yet to be found, ensuring a use for the right purpose as well as avoiding narrowing down the use of data for health outcomes.

Costs and benefits

Below is presented the synthesis of the perceived costs and benefits for the drivers and obstacles identified within this research area, through the impacts of harmonising the rules or not.

Table 7. Data protection and liability drivers

Drivers	Secure access to ePrescription and EHR	GDPR implementation	Codes of conduct to complement the EU Medical Device Legal Framework	Patient mediation through transparency, right information and appropriate consent model	Better regulation guidelines and Product Liability Directive
Impact	++	++	+	+++	+
	---	-	-	--	-

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

Source: Authors' elaboration

Table 8. Data protection and liability obstacles

Obstacles	Highly demanding privacy frameworks	Uncertainty around liability and safety rules	Lack of framework for patients' control over their health data beyond GDPR	Consent model granularity
Impact	--	--	---	---

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

Source: Authors' elaboration

The implementation of complete secure processes for data access remains complex and brings significant costs for the industry in order to ensure compliance. Besides, the fine penalty for the lack of compliance is another major concern for the service providers. In addition, the national authorities have to build specific model (e.g. for consenting) and to dedicate important resources to review the compliance of each provider.

However, such processes increase trust and credibility, since the citizens gain more control over their private data and its usage, demonstrating transparency and responsibility by the provider.

Moreover, data management processes provide standardisation of processing and thus allow the automation of certain actions and thus a reduction in costs. An optimized return on investments can be perceived through opt-in policies and data subject's consent to process personal data: combined with irrelevant information purging and fine-tuned database, the service providers are able to better tailor their message to the specific needs and habits of their consenting users. Furthermore, improved data management and cybersecurity are identified through a better

understanding of the data being collected, as regulation pushes to know precisely the information held on people and to set up adequate administrative and technical measures to protect EU citizens.

The added value of the consistency in the approaches on the use of health data should focus on the benefits it brings to the patients but provide benefits for every stakeholder involved: real “quick-win” benefits are expected through building a health data sharing consent model on specific use cases in a first approach (e.g. rare diseases).

2.2.5 Professional qualifications

Drivers

European initiatives on telehealth professional qualifications. Recognition of professional qualifications is regulated in Directive 2005/36/EC⁷³ on recognition of professional qualifications. This Directive specifies requirements on training duration and acquired medical knowledge and skills for certain health professions that fall under the automatic system of recognition of professional qualifications. However, the provision of digital services in healthcare raises new issues related to professional qualifications, e.g. integration of digital skills and the use of digital technologies in the medical training, as well as continuous professional development. Without providing additional requirements, basic medical training could be recognised with digital competencies and even extended to other professionals apart from most specialist medical doctors. Some initiatives were launched at European level to overcome the scarceness of legal provisions applicable to remote services and to help the effective spread of telehealth into daily practice, such as the eHAction and JASEHN deliverables.

- **JASEHN recommendations on a Common Framework for Mapping Health Professionals' eHealth Competencies**⁷⁴ provide a conceptual framework for eHealth profiles and competencies for addressing all relevant tasks included in eHealth service's lifecycle. Thirty-seven healthcare professionals' profiles were defined group into three areas: health, non-health and IT. For each profiles, mission and main tasks were defined, arranged into six domain areas.
- **WP6 of the eHAction**⁷⁵ focused on eSkills for Professionals and elaborated a competence framework, based on the JASEHN proposition in T7.1.3 Recommendations on a Common Framework for Mapping Health Professionals' eHealth Competencies. The selected framework allows healthcare professionals to self-assess against the full competence framework or against one of the seven health role profiles that are predefined in the model. This methodology was approved thanks to a pilot phase including five EU Member States. **TeleSCoPE** project, launched in 2008 by the European Commission, issued the 'Telehealth Services Code of Practice for Europe' (known as the "Telehealth Code"), an optional instrument for ensuring high quality remote care. Among other recommendations, this code promotes a repartition of tasks among involved professionals (physicians, nurses and private providers) and collaboration of healthcare professionals, developers and patients from design to implementation of telehealth tools (Botrugno, 2019 and Michele Calabro, EPF).
- **"Digital Doc"** project⁷⁶ run by the Erasmus University of Rotterdam is a thematic network under the EU Health Policy Platform. It gathers both thematic networks (healthcare

⁷³ <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32005L0036>

⁷⁴ [JASEHN D7.1.3 RECOMMENDATIONS common Framework mapping health profession....pdf](https://jasehn.eu/sites/jasehn.eu/files/jasehn_d7.1.3_recommendations_common_framework_mapping_health_profession....pdf)

⁷⁵ [ev_20190611_co322_en.pdf \(europa.eu\)](https://ec.europa.eu/health/sites/health/files/policies/docs/ev_20190611_co322_en.pdf)

⁷⁶ https://ec.europa.eu/health/sites/health/files/policies/docs/ev_20191017_co12_en.pdf

professionals organisations) and medical universities confirmation of 17 different MS, 10 pending.

- "**Doctors going digital: How to future-proof skills**"⁷⁷ was a joint conference organised by CPME on the Digital Change in medicine and the required skills/knowledge for doctors. The panel discussion involved six representatives of the eHealth ecosystem.
- **EUHPP Thematic Network - Profiling and Training the Healthcare Workforce of the Future led by the European Health Management Association**⁷⁸ is a thematic network under the Digital Europe program led by the European Health Management Association and Health First Europe. Through a dozen of use cases, their joint statement aimed at defining core digital competencies for doctors by establishing a set of 12 policy recommendations.

In addition, network stakeholders such as HL7, IHE or the eHL project implement educational offers in eHealth through programs including IT knowledge (standards, data exchange, using IHE, EHR, information processing, etc.) as well as medical technology.

Inclusion in healthcare professionals' curricula. The consultation highlighted the specific dynamic nature of digital tools and the need to better train healthcare professionals in order to improve their understanding of eHealth tools, thus their trust, greatly supporting patient education as a result.

Both the representatives of healthcare professionals and the eHealth industry agreed that specific technological trainings should be added to medical curricula, following two different levels: (i) a baseline approach with horizontal topics on digital health (e.g. limitations of technology, digital communication with patients, understanding of telemedicine, smart devices, AI and big data awareness) for the undergraduates and (ii) specific classes with strong digital skills framed according to their medical specialty (e.g. cybersecurity, data protection). MedTech industry stakeholders called for such additional training on cybersecurity and data privacy protection to help them better understand the possible threats, the effects they could have, as well as how to better protect themselves and their patients from these threats. Nevertheless, the industry still expressed concerns about the financing source of such training, worrying that the burden continues to be borne by the industry. The European Commission could have a role in centralising the best practices for Member States.

⁷⁷ <https://www.bundesaerztekammer.de/cpme-2020/digitalskills/>

⁷⁸ <https://ehma.org/euhpp-thematic-network-profiling-and-training-the-healthcare-workforce-of-the-future/>

Box 18. National initiatives for eHealth skills and qualifications of healthcare professionals

Several studies and surveys identified specific digital skills for the provision of healthcare services.

Austria. A survey sent to professionals, medical students, global and European network partners, helped to define specific necessary skills needed for healthcare professionals. Based on the results, the UASTW implemented a specific master's degree, "Biomedical Engineering Sciences" including IHE Basics, IT Infrastructure, Security, Medical Device Connectivity and Clinical Document Architecture (Herzog et al., 2015).

Finland. According to Ahonen et al. (2016), nurses are at the centre of the Finnish eHealth strategy regarding both patient information on available eHealth services and encouraging its use among healthcare professionals. Therefore, nurses' education includes five descriptions of learning areas: learning, ethicalness, working skills, innovations, and internationalism. A similar strategy is observed in the US (Rutledge et al., 2017).

The Netherlands. In 2015, a 51-expert study was conducted to identify required competencies for the development of nursing telehealth education. Among new competencies specifically required when executing telehealth activities, 14 of them appeared to require additional specific soft skills.

Source: Authors' elaboration

Adoption in daily practice and evolution of HPs' roles. National eHealth platform managers mentioned several case laws to stress the fact that consulting a patient's file to avoid medical error is an incentive to use digital services, drawing attention on the fact that patients are more likely to see a doctor using digital tools, benefitting from better quality and more personalisation. For instance, the Belgian eHealth platform has put one operational service online every month and ensured the usefulness of each one for the final user: the main principle decided is not to interfere with the doctors' expertise, having the least impact possible on the daily practice.

It has been highlighted that such adoption would also be fostered through the evolution of healthcare professionals' roles. Since digitalisation is not only a technical change but also an organisational one, this evolution emphasised the need to clarify and specify their new roles in order to build trust regarding eHealth (Cwikilicki et al., 2020). According to HP representatives, a digital leader in healthcare structures is a key role for health adoption, bearing responsibility to introduce the technology to other healthcare professionals, avoiding that the promotion of eHealth only relies on ICT's vendors. Such profiles should have strong competencies in both medicine and technology.

Obstacles

Lack of available trainings and incentives. Such an ambition must be supported by tailored trainings for both healthcare professionals and patients. In a 2019 study (Giunti et al.), the education program of 302 medical schools from each of the 27 European MS were analysed. About a third (90/302) of all medical degree curricula offered any kind of HIT course, dedicated classes were mainly mandatory (58/90). From a national point of view, HIT courses are offered in less than half of the medical schools. The consultation stressed that healthcare professionals current training lacks coherence with regards to the non-binding use of services: as a result, HP are not willing to spend time on training for a non-reimbursed tool.

Lack of effective mutual acceptance of healthcare professionals' competencies. Several stakeholders stressed that mutual professional qualification recognition is not yet settled at an EU level, which highly impacts the provision of telehealth services. A harmonisation of

healthcare professionals' digital skills would start by settling different levels of qualifications to match each Member State status of development in digital healthcare. However, it was also highlighted that this remains a slow process, since some Member States are still struggling with their national accreditation bodies. The definition of an EU accreditation body dedicated to digital healthcare skills could be a way to build a cross-border trust relationship and foster maturity in the field.

The implementation of the Directive 2011/24/EU raised several issues regarding the access of patients' data from professionals of other countries. The main issue arises when the different healthcare providers have not legally the same access rights between two different countries (e.g. nurses, nurse aid, etc.): each contracting party shall ensure that only health professionals authorised according to its national law may have access to patients' data concerning health. Such action should be made without prejudice to other lawful grounds for processing under Regulation 2016/679/EU (Text of Clause II.1.1.3. of the Trade Facilitation Agreement).

Box 19. Example of the Aachen – Maastricht university hospitals collaboration

Directive 2005/36/EC on the recognition of professional qualifications sets a starting point for workforce exchange. Following the introduction of this example in section 2.3, a closer look to the legal dimension showed different contracts to enable professional resources sharing: consultancy-like model (full employment at one hospital and fraction of invoiced time at a partner hospital), dual employment (part-time contracts at both hospitals) and inter-hospital contracts (dispatch to the partner hospital either on an ad-hoc or regular basis). Despite these contracts, staff exchanges were delayed due to long administrative procedures, related to the recognitions of professional's qualification.

Even in border regions, cross-border healthcare collaboration is not a standard practice. However, the University of Maastricht (NL) and Aachen (DE) manage to implement a cross-border top medical program in cardiology⁷⁹.

Source: Authors' elaboration

Costs and benefits

Below is presented the synthesis of the perceived costs and benefits for the drivers and obstacles identified within this research area, through the impacts of harmonising the rules or not.

Table 9. Professional qualifications drivers

Drivers	European initiatives on telehealth professional qualifications	Inclusion in healthcare professionals' curricula	Adoption in daily practice and evolution of HPs' roles
Impact	++	+++	+++
-	-	-	--

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

Source: Authors' elaboration

⁷⁹ [The Aachen-Maastricht Alliance \(healthcare-in-europe.com\)](http://The Aachen-Maastricht Alliance (healthcare-in-europe.com))

Table 10. Professional qualifications obstacles

Obstacles	Lack of available trainings and incentives	Lack of effective mutual acceptance of healthcare professionals' competencies
Impact	--	

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

Source: Authors' elaboration

2.2.6 Online sales of pharmaceutical products

Drivers

Common labelling and authorisation rules. The EU logo for online sales of medicine includes the national flag (Member States, Iceland, Liechtenstein and Norway) and a hyperlink to the national competent authority listing all the legally operating online pharmacies. From the online pharmacies industry point of view, the logo showed its usefulness for tackling counterfeit medicines market (according to a WHO report⁸⁰, almost 50% of medicines purchased online are counterfeit) and the adoption of this logo fosters use and trust on online pharmacies both for patients and healthcare professionals, proving the efficiency of labelling eHealth services at a European level. However, procedures and labelling could be better promoted through EU campaigns. Furthermore, due to linguistic similarities in Europe, the search engines may display results from several countries and increase the exposing to further risks due to a more extensive array of potential distributors of counterfeited medicines (Frangéz et al., 2016).

In France, the online sale of on-prescription medicines' is restricted to online extensions of brick-and-mortar pharmacies⁸¹, under these conditions, reimbursement is applicable and as much as of face-to-face dispensation: regional health agencies (ARS) are responsible for issuing authorisation and for monitoring. Moreover, both ePrescription and eDispensation remain the responsibility of the pharmacist and require interactive exchanges between the patient and the pharmacist, such as verification of personal data (age, weight, height, sex, current treatments, allergic history, contraindications and, if applicable, pregnancy). The USA implemented a certification for online pharmacies, the Pharmacy Verified Websites Program and Digital Pharmacy Accreditation⁸² with 10 principles for online pharmacies. It is entitled to identify safe and legitimate pharmacies. It is currently recognised by 24 state boards of pharmacy. Following the example of both the USA and France, an appropriate national body could grant certification and ensure monitoring of online pharmacies, in relation with European guidance, to tackle the fragmented perspective on online pharmacies regulation.

Advisor role of pharmacists. Despite the extension of pharmacists' role, to management of point-of care tests and vaccination, pharmacists remain the first resort of healthcare services and products, and therefore advising patients is primordial. ePharmacies representatives highlighted that online pharmacists are providing qualitative and safe services through a multiplicity of tools (chat, video/phone call, etc.), given the importance of interaction and personal advice in the pharmacist role. The pharmacist's role is not only to dispense medicines or medical products but also to provide advice, particularly concerning the taking, the use or

⁸⁰ <http://www.newmediatrendwatch.com/markets-by-country/18-uk/148-usage-patterns-and-demographics>

⁸¹ Article L.51215 of "Code de la Santé Publique", 2016 -

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033507633/>

⁸² <https://nabp.pharmacy/programs/accreditations-inspections/digital-pharmacy/#:~:text=The%20Digital%20Pharmacy%20Accreditation%2C%20formerly,growing%20list%20of%20rogue%20websites.>

interaction with other medicines. This advisor role of the pharmacist is often overlooked in online pharmacies (Alwon et al. 2015). In order to counter this lack of interactions, some online pharmacies use a form (Boyd et al., 2017).

Obstacles

Lack of clarity in online pharmacy services definitions. “Telepharmacy” is defined as the delivery of pharmaceutical care to outpatients at a distance using telecommunication and other advanced technologies (Tzanetakos et al., 2017). More precisely, online pharmacies are classified according to the reflection of their online behavior (Frangez et al., 2016): (i) an extension of classic “brick and mortar” pharmacies, where in such cases the online sale of medicine is used to expand the clientele, compete with similar business, etc. (Oliver et al., 2000); (ii) “online-only” pharmacies: these pharmacies are legitimate in nature and they only conduct business online; or (iii) “life-style” pharmacies, potentially rogue site (illegal pharmacies), which offer a narrow range of pharmaceuticals, such as dietary and nutritional supplements, medicines for weight or hair loss, etc. (Jack, 2016).

According to ePharmacies representatives, the definition of online pharmacy’s services and products remains a grey zone in several Member States and EU laws: 27 different definitions of OTC (over the counter) and Rx (prescription) medicines can be found across the European Union. Moreover, while ePharmacies services and ePrescription are interconnected, several countries only support one of the two services: fourteen Member States provide ePrescription, but not online pharmacies and five countries supports only ePharmacies. Last but not least, four countries support both (four Member States support neither ePharmacies nor ePrescription). For instance, German online pharmacies show a good stage of development despite the lack of national ePrescription, which will apply in 2022. ePharmacies industry highlighted the potential added value the EU could provide on ePrescription through the EHDS.

Reluctance from European actors. The industry representatives mentioned that some EU Member States were still reluctant to let ePharmacies into their healthcare system, therefore hampering foreign companies to enter the market by acting against EU laws. For instance, they gave the example of Germany which is applying a fixed price on prescribed medicines (Law on Medicinal Products, Arzneimittelgesetz⁸³) despite the judgment of the European Court of Justice of 19 October 2019⁸⁴, which concluded that the German system of fixed prices at pharmacy retail level for prescription medicinal products is contrary to EU law, since it constitutes a restriction of the free movement of such products between Member States. However, it should be noted that Germany has shown a softer position and anticipation for online pharmacies on other aspects, for instance not asking for face-to-face pharmacist-patient contacts as a condition for dispensing prescriptions. The face-to-face contact needed for giving health advice also stresses the public health considerations in regulating pharmacist-to-patient interaction.

⁸³ [AMPreisV - nichtamtliches Inhaltsverzeichnis \(gesetze-im-internet.de\)](https://gesetze-im-internet.de/ampreisv/)

⁸⁴

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=184671&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=21496650>

Costs and benefits

Below is presented the synthesis of the perceived costs and benefits for the drivers and obstacles identified within this research area.

Table 11. Online sales of pharmaceutical products drivers

Drivers	Common labelling and authorisation rules	Advisor role of pharmacists
Impact	+++	++
	--	-

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

Source: Authors' elaboration

Table 12. Online sales of pharmaceutical products obstacles

Obstacles	Lack of clarity in online pharmacy services definitions	Reluctance from European actors
Impact	--	---

"-": low costs; "--": medium costs; "---": high costs; "+": low benefits; "++": medium benefits; "+++": high benefits

Source: Authors' elaboration

2.3 Current regulatory practices and gaps

2.3.1 Member State approaches

Various levels of digital maturity are observed across the EU, with major differences in the availability of eHealth services and the implementation of regulatory practices. Therefore, it is important to give a picture of the approach adopted by the MS in the scope of regulations and cross-border healthcare. In order to assess how well the MS were performing in this field regarding development of eHealth services, we have identified the most relevant national provisions on telehealth, telemedicine, mHealth and EHR, with the objective to map the Member States' approaches following two levels: (i) Directive 2011/24/EU impacts and (ii) other MS legislation on telehealth/telemedicine, mHealth and digital records/registries.

Current overview of the impacts of Directive 2011/24

Evaluation of Article 14 of Directive 2011/24/EU report analyses the impacts of Directive 2011/24 on patient mobility, availability of EHR at a cross-border level and data portability.

If Article 7 impacts on **patient mobility** were assessed, a 2018 report on MS data on cross-border patient healthcare following Directive 2011/24/EU⁸⁵, provides some insights into actual patient mobility. Requests for information on cross-border care received by National and Regional Contact Points in 2017 accounted to 71,396 cross the 25 NCPs providing data. While most MS received fewer than 1,000 requests, Poland and Lithuania stand out in receiving 30,698 and 14,470 respectively. However, several reports^{86 87} on cross border reimbursement of healthcare has been shared by the European Commission, showing an important increase of

⁸⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52018DC0651&from=EN>

⁸⁶ https://www.europarl.europa.eu/doceo/document/A-8-2019-0046_EN.html

⁸⁷ https://ec.europa.eu/health/sites/default/files/cross_border_care/docs/2019_msdata_en.pdf

these figures. For instance, in 2019, over 6 million reimbursement requests were received by the MS. The total number of requests for reimbursements of patient mobility not subject to prior authorisation was relatively low in all three years before 2017 as a share of total patient care (more details are available in the section of the report on the evaluation of Article 14 of Directive 2011/24/EU). The European Commission estimated that almost half of the EU population has a European Health Insurance Card, and over 2 million request reimbursements yearly. In 2017, there were 17 million EU citizens living in an EU Member State other than their country of citizenship and 1.4 million cross-border workers were active in the EU. However, this data is relevant more generally with regard to the Regulations on the coordination of social security systems, and not only the Directive.

Regarding **electronic health records availability**, the use of MyHealth@EU, although above the forecasted targets, is still very limited in absolute terms. So far only 7 Member States offer some kind of services on the platform. All together, these 7 countries account to 32,997,906 people which represent only 7.38% of the overall EU population⁸⁸. This of course also affects the level of continuity of care for patients after treatments and/or services are provided by healthcare providers abroad. Given the relatively low level of platform usage and cross-border mobility, no major impacts on national healthcare systems were identified. According to Azzopardi-Muscat (2018), the directive did not have a major transformative effect on national health systems. However, this does not allow citizens (not necessarily patients) access their own data across borders. The Directive does not set out any rights of individuals to access/control their health data generated across borders (or nationally), neither through the MSA or MST, but is efficiently complemented by the GDPR.

Although enabling citizens to take an active role in the management of their health was included in the last JA, the impact of article 14 on the access of patients to their electronic health records was limited as no outputs impacting this area were produced. As a result, only a handful of countries provides electronic formats when implementing Article 4.2 (f) and Article 5 (d) of the Directive 2011/24. Only 4 Member States have rules to provide digital access to a copy of the medical record/s for patients affiliated to their healthcare system seeking cross-border healthcare in another Member State (Croatia, Czechia, Greece and the Netherlands) and Finland is planning to implement such rules over the upcoming three years.

In terms of rules to provide digital access to a copy of the medical record/s of received treatment/s for patients affiliated to a different healthcare system that used cross-border healthcare in their Member State, only three countries provide such rules (Germany, Greece and the Netherlands) and three are planning to do so over the coming three years (Czechia, Finland and Poland).

⁸⁸ EUROSTAT 2019 data

Overview by Member State. Below is presented an overview of the answers to the online survey by area, with an estimate of the maturity based on the percentage of positive answers on the existing regulation.

Table 13. Regulatory development

	A1 - Definitions	A2 - Approval, certification, ..	A2 - Practices	A2 - Reimbursement	A2 - Pricing	A2 - HTA	A3 - Interoperability	A4 - Safety, liability and privacy	A5 - Professionals qualifications	A6 - Online Pharmacies
Advanced countries (more than 60% of "Yes" in existing rules questions)	16%	9%	3%	6%	3%	12%	0%	0%	22%	31%
Average countries (from 30% to 60% of "Yes" in existing rules questions)	28%	16%	9%	3%	9%	6%	16%	9%	0%	0%
Advanced countries (less than 30% of "Yes" in existing rules questions)	19%	25%	31%	44 %	12%	3%	19%	37%	0%	0%
No information	37%	50%	56%	47%	75%	78%	66%	53%	78%	69%

Source: Authors' elaboration

Other MS legislation

Telehealth and telemedicine. By the stage of completion of the report, several EU member countries had specifically regulated the telemedicine acts.

In France, teleconsultation, teleexpertise, remote medical monitoring, remote medical assistance and medical response are considered as medical acts, reimbursed by the Social Security fund. In Italy, some elements are excluded from telemedicine such as information portals, social networks, forums, newsgroups, electronic mail or other. (Consiglio Superiore della Sanita – 2017). In Hungary, in the Directive 2020/559/HU, includes within telemedicine the following services: (a) make a diagnosis or recommend therapy; (b) perform counselling or consultation; (c) perform patient management; (d) give referrals; (e) perform care activities; (f) perform therapy and rehabilitation activities; (g) prescribe medications; (h) prescribe therapeutic equipment that can be ordered via ePrescription. In Germany, a new digital Healthcare Act has been introduced which will allow doctors to prescribe digital healthcare applications to patients, which can be reimbursed by the country's statutory health insurance. Application providers will have to prove to the Federal Institute for Drugs and Medical Devices (BfArM) that their applications can improve patient care. Moreover, since 2019, teleconsultation can be provided without any preliminary face-to-face consultation⁸⁹, including psychotherapy.

⁸⁹ <https://mtrconsult.com/news/new-regulation-video-consultations-germany>

To promote telemedicine adoption, the German National Association of Statutory Health Insurance Funds (GKV-Spitzenverband), in coordination with the National Association of Statutory Health Insurance Physicians (KBV) refunds the fee system for teleconsultation, using the respective insured, basic or consult flat rate instead of the fee order item.

Several examples are presented in the comparative analysis of telemedicine legislatives frameworks below, which provides an overview on the issues being dealt with through legislation among Member States and highlighting several differences.

Box 20. Examples of legislative framework for the telemedicine in MS

In order to implement digital health products, Member States often have a use case approach, such as chronic diseases or rare diseases. This approach makes it possible to test products and services on a small and often more voluntary population because they are severely affected. Denmark, for example, has implemented telemedicine services for patients with COPD.

Countries can then extend the most successful services to the rest of the population, as in the case of telemedicine in France, Germany and Italy.

Finally, health crisis episodes, such as the Covid crisis, have lifted certain access limitations, such as the obligation to consult the doctor in person before a teleconsultation

In Denmark, telemedicine is specifically targeted at patients with Chronic Obstructive Pulmonary Disease (COPD) who tend to have frequent visits to a clinic.

In Estonia, since March 2013, consultation of the family doctor with a specialist is reimbursed by the Estonian Health Insurance Fund (EHIF). The specialist provides his instructions for treatment (by e-mail or other means) and receives 68% of the normal rate for a face-to-face consultation (Kruus et al., 2015).

Finland has had a telemedicine strategy since 1995. Teleradiology has become regular practice and is the main telemedicine act in Finland. Most district hospitals provide teleradiology and telelaboratory services and offer teleconsultation for primary healthcare centres. These activities are partially covered by the healthcare system and the budget of the healthcare centres. Other telemedicine services provided are telepsychiatry, teleophthalmology, teledermatology and teledentistry. Most telemedicine projects, focusing on teleconsultation and telemonitoring, were funded by public funds and EU projects (Khatri et al., 2011).

In Germany, according to the professional codes, diagnoses and prescriptions have to be provided after a face-to-face meeting between the patient and the physician and after an examination. Teleconsultations are possible for follow-up purposes and have been eligible for financial compensation since 2017, as have tele-expertise services (Hantson, 2019). Since the ban on tele-therapy only applies if the practising physician is a member of the German medical association (Bundesärztekammer), it does not apply to telemedicine provided by health providers outside the territory (Europe Economics 2019).

In France, teleconsultation has been reimbursed since 2018 at the same rate as a normal consultation, as long as there is a prior therapeutic relationship between the health professional and the patient. Tele-expertise has been funded since February 2019. Two levels of tele-expertise are defined, depending on the complexity of the telemedicine services provided (low difficulty and patient with chronic disease).

In Italy, many telemedicine projects have been initiated but only a few were sustainable. Telemonitoring and teleradiology are considered established practices, while telepathology, teledermatology and telepsychiatry, in the form of teleconsultation and tele-expertise, exist as pilot projects or informal practices (World Health Organization, 2016). Telemonitoring pilot

projects are being implemented at a regional level by the regional health authorities (Azienda Sanitaria Locale, ASL) (Rojahn et al., 2016).

In the Netherlands, since 2019, it has been made easier for health care providers and health insurers to include digital consultations in funding agreements. For GPs it no longer matters how the doctor organizes the consultation with the patient: in the consultation room, by telephone, by e-mail or using other digital means. In specialist medical care it has become easier to fund remote monitoring of patients. Attempts have also been made to implement telemonitoring for heart failure and diabetes in Dutch hospitals (Kroneman et al., 2016; Faber et al., 2017).

In Portugal, a national telehealth strategy and policy was implemented in 2013. One third of hospitals have offered telemedicine services since 2014 (Pina 2015; Dias 2017). Since 2013, the Health System administration has funded several telemonitoring projects. Local authorities have created a certification for teleconsultation. When a teleconsultation is required between a specialist and a patient, primary care units appoint a coordinator or the patient's own General Practitioner to assist during the consultation (Oliveira et al. 2014). More than half of hospitals use remote screening, particularly in the area of dermatology, and have carried out teleconsultations (The Portugal news 2019).

To be noted: in Norway, most telemedicine services are available through projects. There is however a disparity between implementation by the Norwegian government and the actual use of telemedicine (Alami et al. 2017).

Source: Bensemmane et al. 2019

Mobile health. Currently, only a few Member States have implemented a specific certification for non-medical devices such as mobile health applications. While Belgium has a specific certification and certifying body for mHealth apps, it is not ruled by a specific legislation and only led by the Federal eHealth action plan. In Germany, the provision and reimbursement of mHealth apps is strictly regulated by two laws, one for the reimbursement of such services (the Digital Care Act) and one for the definition of the detailed procedure for the certification (Digital Health Applications Ordinance, DiGAV)). The Digital Healthcare Act introduced “app on prescription” for patient into the healthcare system (Section 33a and 139e of the German Social Code Book V). France is currently setting up a personal digital health space under French Health law project “Ma santé 2022”, which is intended to allow exchanges between certified health apps and the national EHR. The Netherlands have asked the National eHealth Living Lab to develop quality criteria for mobile health applications.

Table 14. DiGA⁹⁰

MS	Germany
Covered services	CE marked mobile health applications
Bodies involved	Application for reimbursement
Criteria	<p>Public bodies</p> <ul style="list-style-type: none"> • National medicines agencies (Federal Institute for Drugs and Medical Devices – BfArM) • Technical requirements <ul style="list-style-type: none"> ◦ Security ◦ Fonctionality ◦ Quality ◦ Data protection, data security ◦ Interoperability • Positive care effects <ul style="list-style-type: none"> ◦ Medical benefits ◦ Structural and procedural improvement
Scheme Typology	<p>Certification by the BfArM</p> <p>Digital Healthcare Act (Digitale-Versorgung-Gesetz, DVG) on 19 December 2019</p>

Source: Authors' elaboration

Table 15. mHealth Belgium⁹¹

MS	Belgium
Covered services	CE marked mobile health applications
Bodies involved	<p>Public bodies</p> <ul style="list-style-type: none"> • eHealth agencies (eHealth Belgium, mHealth Belgium), • National medicines agency (AFMPS – Agence Fédérale du Médicament et Produits de Santé), • National sickness fund and insurers (INAMI - Institut National d'Assurance Maladie Invalidité)
Criteria	<ol style="list-style-type: none"> 1. CE-marking 2. Interoperability 3. Socio-economic value added
Scheme	<p>Three-level certification</p> <ul style="list-style-type: none"> • Level 1– basic requirements <ul style="list-style-type: none"> ◦ CE declaration as a medical device is submitted ◦ Voluntary notification of the mobile app to the Federal Agency for Medicines and Health Products (FAMHP), during which the CE marking and the compliance with the rules and regulations for medical devices are confirmed and can be checked. ◦ The app and the parent company declare that they comply with the EU General Data Protection Regulation (GDPR). • Level 2– interoperability criteria <ul style="list-style-type: none"> ◦ Level 1 certified ◦ have been submitted to a risk assessment (developed by an independent organisation and included in mHealthBelgium) after which they have proven to meet all imposed criteria regarding authentication, security and the use of local e-health services by means of standardised tests (if applicable). • Level 3– reimbursement <ul style="list-style-type: none"> ◦ Proof of socio-economic value added ◦ Certification operated by the national social fund
Typology	Framework

Source: Authors' elaboration

⁹⁰ https://www.bfarm.de/EN/MedicalDevices/DiGA/_node.html⁹¹ <https://mhealthbelgium.be/validation-pyramid>

Table 16. ANS eHealth Label

MS	France
Covered services	Software and health establishment
Bodies involved	Public bodies <ul style="list-style-type: none"> National eHealth authority (ANS – Agence du Numérique en Santé)
Criteria	For healthcare professionals and software developers Garanty the basic functions for medical exercise, coordinated care, monitoring, administration of the establishment
Scheme	Label delivered by the French eHealth agency
Typology	Framework

Source: Authors' elaboration

Table 17. HAS mHealth

MS	France
Covered services	Mobile applications with no medical specific purpose Specific for the "grey" zone of mHealth applications
Bodies involved	Public bodies <ul style="list-style-type: none"> National health authority (HAS – Haute Autorité de Santé)
Criteria	Four main axes <ul style="list-style-type: none"> delivering reliable and quality health information, either technically efficient, guaranteeing the confidentiality and security of personal data being ergonomic and easy to use
Scheme	Guidances for mobile applications developers
Typology	Guidelines

Source: Authors' elaboration

Table 18. MAST CIMT

MS	Denmark
Covered services	Telemedicine
Bodies involved	Public bodies <ul style="list-style-type: none"> Centre for Innovative Medical Technology (CIMT). Research center from a university and a university hospital.
Criteria	The model defines the relevant assessment framework for the effect of telemedicine: <ol style="list-style-type: none"> the patient and the technology, patient safety, clinical effectiveness, patient perspectives, economic aspects, organisational aspects, legal and ethical aspects.
Scheme	Assessment framework for managers in the healthcare sector.
Typology	Framework

Source: Authors' elaboration

Digital records, EHR and registries. Through the analysis of the literature (more details are available in chapter 4), the national projects and laws and the consultation phase, we observed that all MS are in the process of developing eHealth strategy with varying level. The first level

being the implementation of EHR, then the development of patient portals and, for most mature countries, developing data management tools to aggregate and analyse data at national level.

The Netherlands are particularly advanced in eHealth development. According to den Exter et al., 2015, an official eID was deployed, as well as making ePrescription compulsory for healthcare professionals. Moreover, several acts were voted to regulate data processing of personal health data (Wabvpz Act), implementation of the GDPR and medical treatment act (Medical Treatment Contract Act, WGBO Act). From a technical point of view, the Act specifies standards to ensure secure data exchanges, NEN7510 and NEN7512, and offers a secure platform to the healthcare providers for data exchanges until they can safely facilitate data exchanges⁹².

2.3.2 Existing EU-level initiatives

List of initiatives

As we identified several obstacles and problems related to digital healthcare provisions, we analyse here the way these aspects are currently governed by existing EU laws and initiatives. This analysis goes through the most relevant provisions at EU level regarding the provision of eHealth services (cross-border healthcare, free movement of services, etc.). The most relevant provisions at EU level are the following:

- *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM (2012) 736 final: eHealth Action Plan 2012–2020-Innovative healthcare for the 21st century.*
- *eHealth action plan 2012–2020 - innovative healthcare for the 21st century.*
- *Report of the Working Group on mHealth Assessment Guidelines.*
- *Draft standard on health wellness apps open for comments – Ehealth standards*⁹³
- *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions European Interoperability Framework – Implementation Strategy COM/2017/0134 final.*
- *Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services, SWD(2012) 414 final—accompanying the document Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, eHealth Action Plan 2012–2020—innovative healthcare for the 21st century.*
- *Draft Code of Conduct on privacy for mobile health applications and CEN ISO work*
- *Medical devices regulations.*

2.3.3 Implementing a European Medical Devices legal framework

Medical devices are products or equipment intended for medical use⁹⁴. Until the adoption of Regulations (EU) 2017/745, Medical Devices Regulation (MDR) and (EU) 2107/746, In Vitro Diagnostic medical devices Regulation (IVDR), medical devices were regulated by Council Directive 90/385/EEC and 93/42/EEC. These two regulations came into effect on 26th May 2017 but will not be applicable until 26th May 2021 for the MDR and 26th May 2022 for the IVDR. The

⁹² <https://www.ploum.nl/en/electronic-access-to-and-copy-of-medical-records-how-can-the-healthcare-provider-meet-its-broader-obligations-under-dutch-law-as-of-1-july-2020/>

⁹³ [Draft standard on health wellness apps open for comments – Ehealth standards \(ehealth-standards.eu\).](http://ehealth-standards.eu)

⁹⁴ <https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices#medical-devices-legislation-section>

MDR, as a gathering and actualisation of two former directives (Council Directives 90/385/EEC and 93/42/EEC), improve the transparency and legibility of the European Legal Framework. The MDR also applies to software and therefore to it is supposed to cover eHealth products (see section 4.2.1. *List of initiatives*).

Box 21. Article 17 of MDR⁹⁵

"17. Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves

17.1. Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.

17.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.

17.3. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).

17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended."

Source: MDR

eHealth Action Plan 2012–2020-Innovative healthcare for the 21st century

The eHealth action plan from 2012 evaluated the development of eHealth and defined the main objectives. In 2012, despite the economic crisis, the telemedicine market was booming, at an annual rate of 18.9% between 2010 and 2011. However, the complexity of the European legal framework was already a heavy burden.

Most of the obstacles hampering the deployment of eHealth at the time are still not addressed, among them: lack of awareness and confidence in eHealth solutions among patients, citizens and healthcare professionals; lack of interoperability between eHealth solutions; limited large-scale evidence of the cost-effectiveness of eHealth tools and services; lack of legal clarity for health and wellbeing mobile applications and the lack of transparency regarding the utilisation of data collected by such applications; inadequate or fragmented legal frameworks including the lack of reimbursement schemes for eHealth services; high start-up costs involved in setting up eHealth systems; regional differences in accessing ICT services, limited access in deprived areas.

The four actions defined to address these barriers were: (1) Achieving wider interoperability in eHealth Services; (2) Supporting research, development, innovation and competitiveness in eHealth; (3) Facilitating uptake and ensuring wider deployment of eHealth; (4) Promoting policy dialogue and international cooperation on eHealth at global level.

⁹⁵ https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_2017.117.01.0001.01.ENG

The first action, interoperability, was supposed to be led by the eHealth network. Through their expertise both on technical aspects and at a MS level, they outcome several guidelines and projects such as the ReEIF (the Refined eHealth European Interoperability Framework), epSOS and addressing the legal issues. eHealth innovation support was included in the "Health, demographic change and well-being" of Horizon 2020 in the following areas: 5P medicine, data valuation for diagnosis, health promotion and cost-effective healthcare.

Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services

This working document from the EU on legal aspects identifies both the legal framework applicable to telemedicine in 2012 and the main legal barriers related to telemedicine services and uses. This working document defined telemedicine as both a healthcare service and an information society service, which corroborates the definition chosen for this study. Therefore, it should comply with laws applicable to these services such as the Directive 2011/24/EU the articles 56 and 57 of the TFEU (Treaty of the Function of the European Union), Directive 2000/31/EC on Electronic Commerce and the Directive 98/34/EC hereinafter the "Regulatory Transparency Directive".

Box 22. Article 56 of TFEU⁹⁶

"Within the framework of the provisions set out below, restrictions on freedom to provide services within the Union shall be prohibited in respect of nationals of Member States who are established in a Member State other than that of the person for whom the services are intended. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may extend the provisions of the Chapter to nationals of a third country who provide services and who are established within the Union."

Source: TFEU

As a service, telemedicine is covered under Article 56 of the Treaty on the Functioning of the European Union. Reimbursement of cross-border telemedicine is regulated in the Directive 2011/24/EU. However, since Member States are obliged to reimburse cross-border carehealthcare if it is among the benefits in the MSA, telemedicine is not always reimbursed. This lack of clarity needs to be addressed in the next propositions.

Box 23. Article 5(2) of the Directive 2005/36⁹⁷

Principle of the free provision of services

"The provisions of this title shall only apply where the service provider moves to the territory of the host Member State to pursue, on a temporary and occasional basis, the profession referred to in paragraph 1. The temporary and occasional nature of the provision of services shall be assessed case by case, in particular in relation to its duration, its frequency, its regularity and its continuity."

Source: Directive 2005/36

As a service of the information society, regulated by the eCommerce directive, healthcare professionals should then be able to exercise if they comply with the rules therein. The multiplicity of applicable European rules to such services makes it even more complex for national bodies to provide the right implementation of the legal framework.

⁹⁶ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12008E056:en:HTML>

⁹⁷ <https://eur-lex.europa.eu/legal-content/en/TXT/HTML/?uri=CELEX:32005L0036>

Interoperability Framework – Implementation Strategy (2017)

The Interoperability Solutions for European Public Administrations (ISA) programme (2010-2015), and its successor the ISA² programme (2016-2020), are the main instruments through which the current European interoperability strategy and European interoperability framework have been implemented. This has involved a variety of actions that aimed to improve digital collaboration between public administrations in Europe.

The interoperability framework was created in response of the need of more specific guidance on how to improve governance of their interoperability activities, establish cross-organisation relationships streamline processes supporting end-to-end digital services, and ensure that existing and new legislation do not compromise interoperability efforts. These recommendations should help public administrations to:⁹⁸ (i) improve their national governance of interoperability activities; (ii) use common operational models to develop better digital public services and include the needs of citizens and businesses from other EU Member States; (iii) manage data they own in common semantic and syntactic formats to make it easier to publish it on portals, and to aggregate, share and reuse it.

The new European interoperability framework puts more emphasis on how interoperability principles and models should apply in practice and considers emerging policy-related and technological needs. The 47 Recommendations are made more specific to facilitate their implementation. There is a stronger focus on openness and information management, data portability, interoperability governance and integrated service delivery. It has been shaped in close collaboration with the Member States and following a wide consultation process with all other relevant stakeholders. Its successful implementation will require the active involvement of all actors, especially public administrations. The planned actions will ensure that the new European interoperability framework can achieve its ultimate objective of interoperable user-centric public services in the EU.

Focus areas of the Interoperability action plan include (details in Annex 7.9): ensuring governance, coordination and sharing of interoperability initiatives; developing organisation interoperability solutions; engaging stakeholders and raising awareness on interoperability; developing, maintaining and promoting key interoperability enablers; developing, maintaining and promoting instruments that support interoperability.

Commission recommendation (2019) on a European EHR exchange format

This recommendation provides guidelines for setting up a European EHR Format in order to achieve secure, interoperable, cross-border access and exchange of health data in Europe. This recommendation is relevant for EU countries as well as for EEA countries (European Economic Area, ie Iceland, Liechtenstein and Norway). This framework sets principles, technical specifications and a process to take forward the elaboration of European EHR exchange format. The EC incent MS to use the tools provided by the eHDSI (eHealth Digital Services Infrastructure) and to refer to the Refined eHealth European Interoperability Framework. Moreover, the Commission defined five baseline data types that should be available in European Patient EHR: (a) Patient Summary, (b) ePrescription/eDispensation, (c) Laboratory results, (d) Medical Imaging and reports and (e) Hospital discharge report. On an organisational point of view, MS should develop a National digital health network including four existant national bodies: (a) the national representative of the eHealth Network; (b) national, or regional, authorities with clinical and technical competence for digital health matters; (c) supervisory authorities established under Article 51 of Regulation (EU) 2016/679; (d) competent authorities designated pursuant

⁹⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A134%3AFIN>

to Directive (EU) 2016/1148. mHealth is an important topic for the Commission policy on eHealth, especially issues around the validity and reliability of data from mHealth solutions.

Draft Code of Conduct on privacy for mobile health applications (2017)

The Privacy Code of Conduct on mobile health (mHealth) apps, facilitated by the European Commission, intends to promote trust among users of mHealth apps, and will provide a competitive advantage for those who sign up to it in the future. The first versions of the Code of Conduct for mHealth apps were prepared against the background of the European Commission's 2014 mHealth Green Paper consultation, which revealed that people often do not trust mHealth apps because of privacy concerns. Following this consultation, the European Commission encouraged industry stakeholders to create a code of conduct on mobile health apps, covering privacy principles, in order to increase trust among users. The Draft Code of Conduct includes practical guidelines for app developers (see details in Annex 7.10).

On 11 April 2018, the Article 29 Working Party⁹⁹ published its assessment, finding that - in view of the entry into force of the GDPR on 17 April 2016, with the application on 25 May 2018 - the criteria of the GDPR should be applied, and that the existing Code did not yet adequately address these requirements. As a result, there was no formal approval of Codes by Article 29 WP under Directive 1995/46. The Commission is engaged with a range of industry stakeholders in order to encourage the further development of the current draft Code, so that it may be submitted to the European Data Protection Board in the future to seek a formal approval¹⁰⁰.

2.3.4 Legislative Inhibitors

Fragmentation and complexity in approval, certification and reimbursement. Legal obstacles are due to the lack of clarity in European legislation on products and services other than medical devices, the complexity of market approval, data protection, liability and reimbursement issues. In addition, demonstration of results is necessary to establish the quality and effectiveness of eHealth, but some stakeholders are dissatisfied with the sensitivity, validity and reliability of existing outcome measures. There is a global lack of understanding of the standards used in the design, production and implementation of the software and hardware that should be used in remote monitoring systems for instance.

Lack of common health data processing and liability frameworks. Despite the new rules on data protection introduced by the GDPR, Member States have different level of expectations on the matter. This variety of expectations between the Member States prevent the development of cross-border products and services, particularly in terms of mobile applications and the transfer and storage of personal data (Health data host certification in France, German Privacy Act). The implementation of EHRs, which is under way in almost all Member States, is a good example to analyse the differences in legal attitudes towards privacy in member states.

Lack of sufficient incentive measures for interoperability. The multiplicity of eHealth providers among the Member States, especially private providers, result in several gaps in interoperability between different telehealth, mobile health and registries systems. It creates a significant barrier which, if not addressed, will lead to continued fragmentation, even more with the mHealth market. Moreover, cross-border interoperability has no binding requirement for infrastructure and information technology in the different certification schemes, despite the recommendations on a European EHR exchange format (2019) and the need to process information consistently across different health information systems, regardless of their

⁹⁹ http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51416

¹⁰⁰ <https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps>

technology, application or platform, in such a way that it can be interpreted in a meaningful way by the recipient.

Lack of healthcare professional digital skills. Even though Member States legislation generally followed the development of ICT in healthcare services, professional trainings didn't. Only few Member States integrated ICT courses in their curriculum, and even fewer have a legal framework regulating the required professional skills. The absence of European regulation is an obstacle to a minimum level of quality for digital healthcare services.

3. Artificial intelligence in health

3.1 Scoping the field

3.1.1 Definitions and techniques

The possibility that a machine could learn from its own experiences and solve problems, conceptualized by Alan Turing in the 1950s as "Computer intelligence", is the precursor of the concept and discipline created by John McCarthy and Marvin Minsky as Artificial intelligence (AI). During the "Dartmouth Conference" (in 1956), McCarthy and Minsky, the fathers of AI, defined Artificial intelligence as "the science and engineering of making intelligent machines, especially intelligent computer programs" (McCarthy, 2007; Angehrn, 2020; Shinnars et al, 2020).

Currently, no universally accepted definition exists and there is no clear consensus regarding a common definition of AI in general and, particularly, in the healthcare domain. Recently the European Parliament provided a concise and helpful general definition for AI, defined as "*the capability of a computer program to perform tasks or reasoning processes that we usually associate with intelligence in a human being*" (Rossi, 2016). More recently, on April 21, 2021, the European Commission published a draft regulation to govern uses and application of AI within the European Union. Article 3 point 1 provides the definition of 'artificial intelligence system' (AI system) as "*means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*". AI techniques and approaches referred to in Article 3, point 1 are the following:

- a) *Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;*
- b) *Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;*
- c) *Statistical approaches, Bayesian estimation, search and optimization methods.*

The categorization of AI range of techniques can be summarized in three main groups: the classical **Machine Learning (ML)**; the recent **Deep Learning (DL)** techniques within artificial neural networks (ANN); and **Natural Language Processing (NLP)** and its associated Natural Language Generation (NLG) methods.

Machine Learning (ML) is defined as "*a field of AI where computers learn automatically from data accumulation*" and it has been extensively applied for big data analysis (Pesapane et al., 2018). ML emphasizes the learning aspect of intelligence by developing computer programs that can "*learn and improve from experience without being explicitly programmed*". In this sense, it has as a reference the brain functioning attempting to imitate neural networks (Abhimanyu S. Ahuja, 2019). The use of machine learning algorithms is growing rapidly in recent years within the healthcare sector providing solutions for early diagnosis, targeted treatments, clinical decision making, perform population-based risk prediction analytics, interpretation of medical data, service organization (e.g., flow optimization, triage, and resource allocation), and patient management and follow-up (e.g., drug administration and compliance) (Rowley et al, 2019; Esmaeilzadeh, 2020).

The capacity of AI-based systems to provide predictions, coming from a classification of patterns, is possible thanks to the use of large medical datasets to train the algorithms. The digitalization

of information in different domains and inherent availability of digitalised data has led to the problem on how to manage and use this data for different applications. These large datasets, sometimes coming from different sources, need the use of computerized mechanisms to process them. Here is where algorithms come to play a decisive role. Some machine learning systems could learn and modify its outputs, they are systems that by successive and repetitive processing of data have the capacity to increment its mode of treatment and to continuously improve its performance (Diebolt et al., 2018). These systems are called **Self-learning** systems.

The learning process of machine-learning algorithms can be divided in supervised, unsupervised, and semi-supervised (a hybrid between supervised and unsupervised learning). **Supervised learning** mainly focusses on classification and prediction producing a known output of a training set, meaning that the tasks performed by the algorithms can be performed also by a trained person (e.g., clinician) and their output approximate human performance. Supervised learning is most used for healthcare applications because it provides more clinically relevant results based on computer high accurate approximations of clinical data like medical images (e.g., X-rays, EEG), electronic health records (EHR) information, environmental and behavioural data, etc. (Deo, 2015; Macrae, 2019; Jiang et al, 2017; Gruson et al, 2019). Examples within the healthcare domain include automated interpretation of healthcare data through pattern recognition from a limited set of diagnoses (e.g. cardiology interpretation of EKG); the automated detection of unusual objects such as lesions categorizing them into groups (e.g. in radiology the categorization of normal or abnormal, lesion or non-lesion patterns); and the estimation of risks to guide therapies, care plans and treatments across different disciplines of medicine (e.g. RiskCardio system that estimates the potential of cardiovascular death from uses ECG signal¹⁰¹).

In the case of **unsupervised learning**, no outcome variables are produced for prediction. Instead, the objective is to find occurring patters or groupings within the data sets. The potential of unsupervised learning in healthcare comes from its application in “precision medicine”, where it can provide the mechanisms to deliver new paths to therapy from heterogeneous conditions. For example, in cardiology, unsupervised learning can be used to characterize and identify the patterns of cellular composition in patients with apparently similar symptoms and characteristics but with unexplained acute heart failure events. Other examples are the use of unsupervised learning algorithms focused on genomics, for instance to identify of subtypes of diseases (e.g. eosinophilic subtype of asthma) that only respond to one type of therapy (e.g. novel therapy with eosinophil-secreted cytokine interleukine-13); and drug discovering and manufacturing. The contrast with supervised learning, is that there is not predicted outcome coming from the characterization of patterns of cellular composition or the identification of subtype of diseases (Deo, 2015).

Deep Learning (DL) is defined as “*a technique, at the cutting edge of machine learning that enables a machine to independently recognize complex concepts from complex datasets, such as elements in images*” (Gómez-González et al, 2020). DL is in turn part of a broader family of ML methods based on ANN with feature learning, that is capable of delivering a higher level of performance and does not require a human to identify and compute the discriminatory features for it (Ho et al, 2019). In addition, deep learning models scale to large data sets, always considering the capacity of the computer hardware used for their execution. DL systems can accept various types of data as input, an aspect of particular relevance for heterogeneous healthcare data (Esteva et al, 2019). Particularly, DL is used in healthcare mainly for medical

¹⁰¹ RiskCardio (MIT). Accessible via: <https://news.mit.edu/2019/using-machine-learning-estimate-risk-cardiovascular-death-0912>

imaging solutions (e.g. diagnosis using MRI scans, CT scans, and ECG), drug discovering, and chatbots that can identify patterns in patient symptoms (in combination with NLP). This technique also allows healthcare professionals to perform classification tasks such as detecting patterns in medical images, define risk-based cohorts of patients with same or analogous characteristics, or establish relationships between symptoms and outcomes from large amounts of unstructured data. In particular, for the diagnosis through medical images, the training of DL algorithms is done by sourcing millions of medical images that have not been labelled by humans. Also, algorithms can help dermatologists make better diagnoses, for example detecting 95% of skin cancers by learning from large sets of medical images (Horgan et al, 2019). The output of DL algorithms is a combination of learning algorithms and formal neural networks which are flexible mathematical models that use multiple algorithms to identify complex nonlinear relationships within large datasets. This probabilistic way of transforming data into 'knowledge' as the basis for a 'prediction' is what it is referred to as 'clinical decision-making' (Gómez-González et al, 2020; Lai et al, 2020; Schönberger, 2019).

Furthermore, **Natural Language Processing (NLP)** is defined as a specialized application using ML ANN and/or DL, and computational linguistics, enabling computers to understand and process human languages and to get computers closer to a human-level understanding of language. On the other hand, Natural Language Generation analyses, interprets, and organizes data into plain, written text or audio output. Thus, Once NLP unlocks the context hidden in data and translates it into human language, NLG takes the output and analyzes the text in context. Sequential NLP is powered in healthcare domain for the standardization of Electronic Health Records (EHRs) information by transforming the free text into standardized data (Jiang et al., 2017). Under this context, NLP targets at extracting useful information from the narrative text to assist clinical decision making. Adapted to EHRs, this technique could translate a patient-professional conversation directly into a transcribed text record. NLP comprises two main components: (1) text processing and (2) classification. Through text processing, the NLP identifies a series of disease-relevant keywords in the clinical notes based on historical databases. Then a subset of the keywords is selected through examining their effects on the classification of the normal and abnormal cases. The validated keywords then enter and enrich the structured data to support clinical decision making. The key challenge lies in ranking the attributes and status of each medical entity from the conversation while accurately summarizing the dialogue (Esteva et al, 2019; Jiang et al, 2017). One of the most significant application of AI in the clinical aspects of healthcare delivery is the domain of "expert systems". These applications use the DL processes to analyse stored knowledge to deduce and provide options (i.e., alternatives, suggestions, advice) to healthcare providers mainly through "if/then" rules to a question/problem. Thus, this human interface activity is communicated "provider to computer" via NLP processing and "computer to provider" via NLG (Arsene et al, 2014).

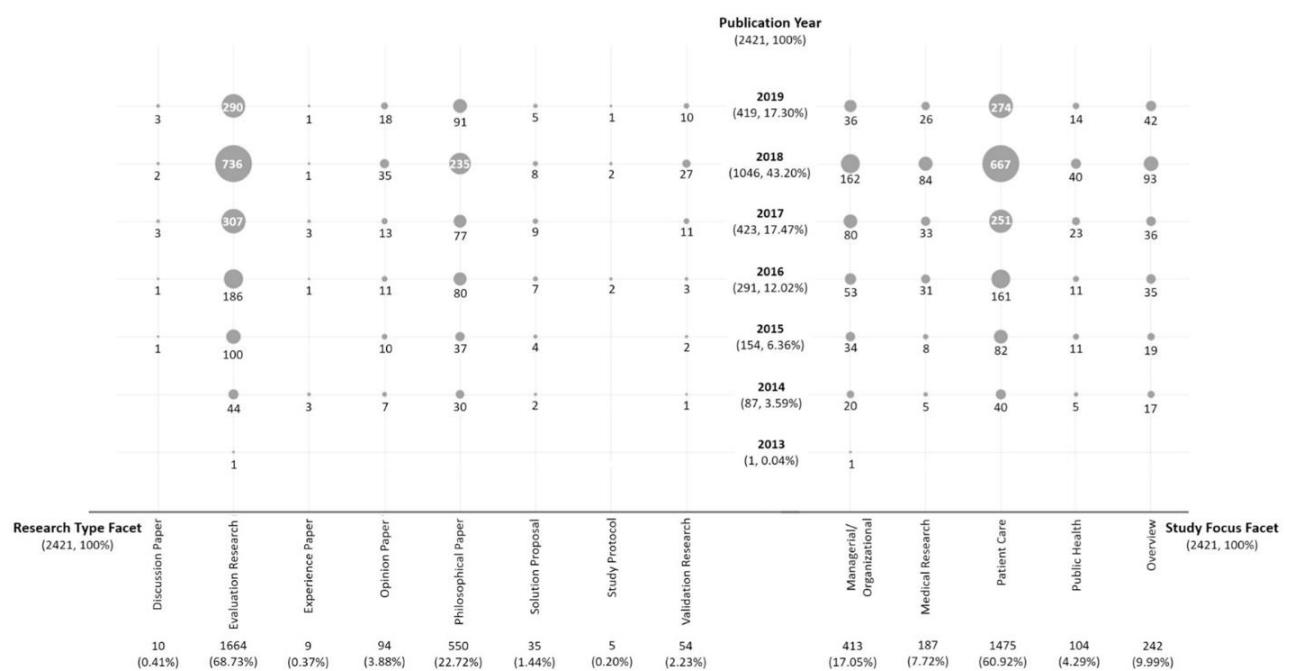
The complexity of the techniques briefly described above has made the concept of "**Explainable AI**" important (Arrieta et al, 2020). The term refers to methods and techniques in the application of AI to make the results of the solution understood by human experts. Explainability is associated with the notion of explanation as an interface between humans and a decision maker that is, at the same time, both an accurate proxy of the decision maker and comprehensible to humans (Arrieta et al, 2020). It contrasts with the "**black box**" concept (cf. Expert Group on Liability, 2019), that can lead to a lack of acceptance by experts and which is increasingly associated with ML. Importantly, there appears to be a trade-off between the performance of a model and its transparency (Arrieta et al, 2020). Some concerns have been raised as AI techniques could foster the growth of "black box medicine", where clinical decision making becomes increasingly opaque and do not easily lend themselves to human concepts of

explanation and significance, while its outputs are typically probabilistic and sometimes inscrutable.

3.1.2 Areas of AI use and levels of control in healthcare

AI could contribute to the financial sustainability of the healthcare system by providing solutions for the management of complex patient's treatment and care needs, as well as complex and large volumes of information. AI use in healthcare has the potential to transform how care is delivered from the clinical point of view but also from an administrative perspective reducing the costs and expenditures of the healthcare systems (Fernández García et al, 2020). AI can play a vital role in the healthcare practice with endless possibilities and powerful applicability. A recent systematic mapping study (Mehta et al, 2019) shows an increased number of publications in the field of AI covering a wide range of research methods ("Research Type Facet") focusing mainly on patients care, managerial and organisational aspects, medical research and public health.

Figure 2. Systematic map of research type and study focus



Source: Mehta et al. (2019)

The following table summarises the main categories and sub-categories identified in the last years. These areas were covered considering many clinical specialities, health policy and health service research as well medical research and software or mathematical modelling.

Table 19. Main areas of healthcare

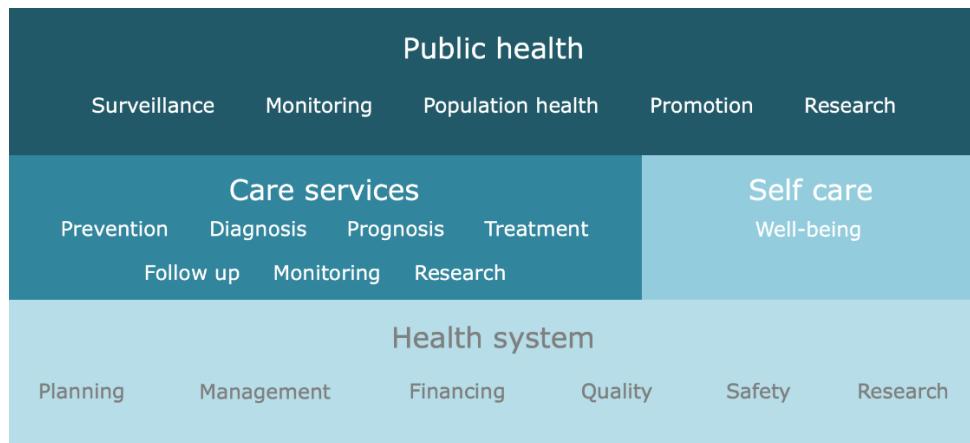
Category	Description	Sub-categories
Managerial / organisational	Studies which focus on administration and management of healthcare services (organizational or broader level)	<ul style="list-style-type: none"> • Big Data Analytics Technologies & Techniques • Data Management • Health Regulations • Health Insurance • Financial Management • Healthcare Operations • Healthcare Education • Healthcare Business Value • Managerial Implications • Information Technology Management • Human Resource • Security, Privacy and Data Ethics • Strategic Planning • Supply Chain Management • Pharmaceutical Management • Systems Management
Medical research	Studies which include clinical research, pre-clinical research and basic medical research.	<ul style="list-style-type: none"> • Artificial Organs • Clinical Research • Biomedical Research • Image Processing & Analysis • Genetics • Drug Discovery and Development
Patient Care	Studies which concentrate on the services rendered (direct or indirect) for the benefit of patient and also studies considering patient healthcare expenditure.	<ul style="list-style-type: none"> • Decision-support • Disease Management • Patient Safety • Pathological Analysis • Image Processing & Analysis • Signal Processing & Analysis • Remote Healthcare • Personal Health Assistance • Therapeutic Management
Public Health	Studies which focus on the entire spectrum of health and wellbeing of the communities.	<ul style="list-style-type: none"> • Disease Surveillance • Health Literacy • Epidemiology • Environmental Epidemiology • Public Health Evaluation and Management
Overview	Studies which discuss about different areas of healthcare or the overall healthcare service delivery, or those which gives the outline about application of emerging technologies for a particular disease or clinical specialty.	

Source: Mehta et al, 2019

Some of the **patient care** where AI-based solutions are most frequently used (Davenport et al, 2019; Horgan et al, 2019; Shinnars et al, 2020; Paranjape et al, 2020, Alami et al, 2020; Biundo et al, 2020) are: (1) **Diagnosis, prognosis and treatment**, providing recommendations and evaluations for different purposes such as early detection of diseases using clinical data, treatment response, identification of common diseases with EHR data and expert knowledge, and **image recognition** for the diagnosis and screening of diseases through image data. (2) **Patient engagement, adherence, management and follow-up** promoting patients' engagement and adherence to treatments and therapies and self-management of their disease, by using personalized information systems for healthy lifestyle promotion, early detection of symptoms, and public education and (3) **Clinical decision-making** process, incorporating (i) **predictive** analytics that lead to obtain precision medicine outcomes, clinical risk interventions and population health information; (ii) **screening** and optimization of **clinical pathways**; and (iv) pathology **classification** using date-driven precision medicine for the delivery of treatments

and therapies, prediction of risk factors, screening, and classification of health-related markers and symptoms. Thus, AI is currently covering a wide range of health areas, including public health, care services, self-care and health systems (see Figure 3). Both primary and secondary use of data play a remarkable role (see chapter 4)

Figure 3. Main areas AI in health



Source: Authors' elaboration

Box 24. AI systems in health proposed definition

Taking into account the definition of health as "*a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity*"¹⁰², and the AIA proposed definition AI systems in health could be defined as *means software that is developed with one or more of the techniques and approaches related to ML; DL and NLP for a given set of human-defined objectives in the areas of physical, mental and social well-being, generate outputs as content, predictions, recommendations, or decisions influencing the environments they interact with, including public health, health and care services, self-care and health systems.*

Source: Authors' elaboration

The level of control of AI is as important as the area of usage. In view of this independence of control, three models of systems have been postulated according to the degree of human-machine interaction (Harbers, et al. 2017; Miro, 2018):

- (1) **Man in the loop**, when the AI needs human contributions at regular time intervals to be able to carry out his actions;
- (2) **Man on the loop**, if the machine is capable of acting by itself based on a previous programming, but the human can intervene by interrupting or modifying the robot's actions at any time; and
- (3) **Man out of the loop**, a model in which the machine acts independently during certain periods of time and, in these intervals, the human being has no influence on the actions of the robot. As can be seen, much emphasis has been placed on the duration of the intervals in which there is human intervention or control and in which there is not.

¹⁰² Preamble to the Constitution of WHO as adopted by the International Health Conference, New York, 19 June - 22 July 1946; signed on 22 July 1946 by the representatives of 61 States (Official Records of WHO, no. 2, p. 100) and entered into force on 7 April 1948. The definition has not been amended since 1948.

This spectrum has been further elaborated according to the health domain. Ng (2021) has identified five levels, including an example related to X-ray:

- **Human only:** No AI involved.
- **Shadow model.** A human doctor reads an X-ray and decides on a diagnosis, but an AI system shadows the doctor with its own attempt. The system's output does not create value for doctors or patients directly, but it is saved for analysis to help a machine learning team evaluate the AI's performance before dialing it up to the next level of automation.
- **AI assistance.** A human doctor is responsible for the diagnosis, but the AI system may supply suggestions. For example, it can highlight areas of an X-ray for the doctor to focus on.
- **Partial automation.** An AI system looks at an X-ray image and, if it has high confidence in its decision, renders a diagnosis. In cases where it's not confident, it asks a human to make the decision.
- **Full automation.** AI makes the diagnosis.

These degrees of autonomy could be applied to any type of AI within in health domain (see Figure 3) with implications not just for the health professionals but also for patients and other stakeholders involved in the provision of the services (e.g. health authorities, health services providers).

The level of control is linked to one of the main characteristics of the health sector: **asymmetry of information** (Arrow, 1963). This makes health domain different from other sectors where AI is applied (e.g. automatic vehicles). Asymmetry of information between actors (specially between health professionals and patients), though not unique to this market, is sufficiently important to have led various institutional arrangements from the doctrine of informed consent to medical malpractice (Sloan, 2001). Within this context, the use of AI in health and the different the spectrum of control reverberates not just the asymmetry of information between health professionals and doctors but also between the outcome of AI systems and the individuals involved in its utilisation. As stated by Arrow (1963) "*demand for medical service is associated, with considerable probability, with an assault on personal integrity. There is some risk of death and a more considerable risk of impairment of full functioning*". In addition, "*because medical knowledge is so complicated, the information possessed by the physician as to the consequences and possibilities of treatment is necessarily very much greater than that of the patient, or at least so it is believed by both parties. Further, both parties are aware of this informational inequality, and their relation is coloured by this knowledge*" (Arrow, 1963).

Despite the evolution of health systems and the explosion of the availability of information (Haas-Wilson, 2001), Arrow's statements are still valid. Therefore, when considering AI in the health domain is very important to consider the **level of expertise** of the actors involved (Prior, 2003), due to the characteristics of the asymmetries of information in healthcare, as well as the **type of results** produced by the AI system (Bitterman et al, 2020; Vellido, 2019; LaRosa et al, 2018; Shinnars et al, 2020; Gerke et al, 2020):

- Based on the level of expertise, two typologies could be defined. On the one hand, the qualified individuals with **expert knowledge** in the field (e.g., doctors, nurses, managers...). On the other hand, non-qualified individuals with **lay knowledge** in the field (e.g., mainly patients and citizens).
- Based on the type of results produced by the AI system two broad categories could be defined: the **provision of information** (e.g., decision support systems, alert systems...) and the performance of a **specific task or activity** (e.g., codification, billing...).

The combination of these elements allows us to create four types of AI systems. Each type could be further divided depending on the level of control. The following figure sketches this typology.

Figure 4. AI systems typology

	Type 1	Type 2	Fully automation Partial automation AI assistance Shadow mode	
Task or activity				
AI system outcome			Fully automation Partial automation AI assistance Shadow mode	
Information	Type 3	Type 4	Level of expertise / qualification	
	Knowledge expertise (qualified)	Lay expertise (non-qualified)		

Source: Authors' elaboration

Type 1. AI systems performing tasks or activities for individuals with knowledge expertise (qualified). AI systems performing tasks by themselves are not yet routinely introduced into the medical practice, although in research, preclinical testing carried out under ideal conditions have been performed. Currently, this validation is insufficient because the AI systems will need to function together with other software, hardware, and highly variable end-users in the real-world setting (Bitterman et al, 2020).

Due to the current trends of using AI in the healthcare sector, medical tasks such as the ones performed by surgical robots have started to consider the incorporation of AI techniques. For example, the Da Vinci Medical Robot is investigating the use of AI to minimize or eliminate the risk of human error. The key point is to reach autonomy of surgical robots centred in the data provided to the robot to perform medical procedures. An example of is the "Verb Surgical Medical Robot" created by Google and Johnson & Johnson¹⁰³. Verb uses advanced imaging, data analysis, and machine learning to enable greater efficiency and improved outcomes across a wide range of surgical procedures such as open surgery and minimally invasive surgery (e.g., laparoscopic, kidney transplant, bypass). In these cases, fully automation is not considered but different levels of partial automation and AI assistance are envisaged.

Care services are not the only health domain that could be included in this type of AI systems. There are cases in the Health system and Public health areas related to the utilisation of NLP to codify EHR or to process claims. For example, preauthorisation processes require the constant presence of a preauthorisation reviewer, which increases the operating expenses of the Health Insurance Providers (HIP). A novel AI technology was able to learn the preauthorisation process using an existing database of a non-profit HIP. The decision-support tool developed can be used to support the activities of the professionals and automatically evaluate less complex cases, like

¹⁰³ Verb Surgical Medical Robot: <https://spectrum.ieee.org/automaton/robotics/medical-robots/google-verily-johnson-johnson-verb-surgical-medical-robots>

requests not involving risk to the life of patients (Araújo et al, 2016). It works in a "Partial automation" level, as it may deny authorisation, but also authorise with high or low level (i.e., requiring professional action).

Type 2. AI systems performing tasks for individuals with lay expertise (no-qualified).

This type of AI system falls mainly under the area of self-care and well-being. For example, the utilisation of wearables, sensors and IoT are facilitating the appearance of services related to fall prevention and/or fall detection, which under specific circumstances, these AI systems may perform a task (e.g., calling assistance services). This type of AI systems could be especially relevant for Ambient Assisted Living (ALL) technologies.

Manogaran et al. (2018) reported the use of IoT sensors for monitoring the patient's health conditions (e.g., respiratory rate, heart rate, blood pressure, body temperature and blood sugar). Once the data is stored in the cloud, the proposed IoT-based health monitoring system uses ML for developing the prediction model for heart disease. It works as a fully automated system as it may perform specific tasks (e.g., calling an ambulance) or require further assistance (i.e., request an incoming supervision call). This type could also cover AI systems which provide treatment to patients: an AI-based artificial pancreas for patients with type 1 diabetes.

Type 3. AI systems providing information to individuals with knowledge expertise (qualified). AI systems that retrieving, processing and analysing information, using existing EHR, clinical databases or data from a device, and present it in a structured way to the individuals taking a decision. These systems help healthcare professionals to make decisions (e.g., diagnosis, best treatment option, detect risk factors, prevention and early detection, etc.) towards a better and comprehensive evidence-based decision-making process, improved health outcomes and healthcare management. In this category, ML and DL techniques with supervised learning are used to provide predictions and provide accurate information for the healthcare professionals. For example, Meyer et al. (2018) developed an AI system using deep learning methods to predict severe complications (i.e. renal failure, bleeding, or mortality) during critical care in real time after cardiothoracic surgery. This "partial automation" AI system triggers the attention of the health professionals towards patients with higher risks. "DeepCare" is an illustration of an AI-based platform working between "Partial automation" and "Full automation" levels, for processing of electronic medical records (EMR) in care services (Pham et al, 2017). It uses a deep dynamic memory neural network to read and store experiences and allows capturing long-term dependencies. Using the stored data, the framework of "DeepCare" can model disease progression, support intervention recommendation, and provide disease prognosis based on EMR databases. Studying data from a cohort of subjects with T2D and mental health patients it was demonstrated that "DeepCare" could predict the progression of disease, optimal interventions, and assessing the likelihood for readmission (Pham et al, 2017).

There are also examples in the area of public health. In surveillance settings, SENTINEL has been designed as a newly developed software system for real-time syndromic surveillance based on social media data (i.e., Twitter, news data, and Centers for Disease Control and Prevention (CDC)) (Serban et al, 2019).

Other platforms have been created specifically for people with dementia. A novel AI approach, for supporting the physical well-being of people with dementia, analyses raw observations and measurement data alongside environmental data, collected from their homes, and generates personalised notifications based on patients' needs, allied to the parameters set by the clinical team. This information is constantly monitored by a group of healthcare practitioners who take appropriate decisions by following a clinical algorithm taking into account the collected data and generated notifications (i.e., actionable information). At the same time, the monitoring team

validates the generated notifications, and this information is used for the evaluation of the developed machine learning techniques (Enshaeifar et al, 2018).

Type 4. AI systems providing information to individuals with lay expertise (non-qualified). It also includes AI systems to support care delivery through patient's monitoring, for example, systems that collect information from a device and present information to patients for self-management of their health conditions (e.g., patient counselling chat bots, wearable devices monitoring vital signs, personalized systems for treatment adherence follow-up). This kind of AI system mainly aims to provide timely and accurate care, some of them incorporating warning systems to notify healthcare professionals in case of risks of health status deterioration or adverse events ("AI assistance"). AI techniques used within this category are ML and DL for collecting and classifying the information for monitoring patient's health status, as well as to provide predictions and recommendations for self-management of their health conditions based on the data collected and analysed; and NLP/NLG for chatbots and automatic patient counselling tools. Another example recently approved by the FDA is Current Health's AI wearable device that measures multiple vital signs at home use¹⁰⁴.

3.1.3 AI development and implementation

The implementation of AI in healthcare is enabled by the current availability of massive health-related data coming from patient's EHR, diagnostic results, and clinical studies. AI systems could replace humans precisely because not only can they outperform them in the final physical execution stage, but they can also automatically access and collect vast amounts of information from various sources, of a magnitude that the human brain could not read in decades (Chagal-Feferkorn, 2019). These algorithms can then analyse these enormous amounts of information that are beyond a human's grasp and can make complex decisions based on probabilities that a human cannot even weigh.

A key feature underpinning the excitement behind AI and ML is their potential to analyse large and complex data structures to create prediction models that personalise and improve diagnosis, prognosis, monitoring, and administration of treatments, with the aim of improving individual health outcomes (Collins & Moons, 2019). Nevertheless, the low availability of data coming from different sources (multimodal data) of a wide number and diverse types of patients and the adequate treatment of this data is leading to problems when developing valid algorithms (Van Hartskamp et al, 2019). Key stakeholders such as healthcare professionals, payers, and government authorities are interested in the generation of real-world data by using AI to facilitate the decision-making process and the development reliable AI applications for medical use, hence the importance of the availability and quantity of health-related data sets. Developers must generate, assemble, or acquire the tremendous data sets needed to train their algorithms; they must assemble the expertise and resources to actually develop those algorithms; and they must validate them to make sure they work (Price, 2019).

In this sense health-related data used to develop AI-systems should be increasingly available and, accordingly, a workflow that covers the overall lifecycle for the development of AI algorithms should be well-defined and established, from the problem definition and requirements elicitation, to selection and preparation of the data, to model design, implementation and training process, and finalizing with the validation and verification of the model and its evaluation in real-world monitoring scenarios. The following phases need to be normalized, standardised, and eventually regulated in order to enable reliable use of AI in healthcare:

¹⁰⁴ Current Health's AI wearable: <https://www.docwirenews.com/docwire-pick/future-of-medicine-picks/first-ai-wearable-approved-by-fda-for-home-use-monitoring-vitals/>

1. Objectives, purpose and requirements elicitation. This phase is referred to the definition and formulation of the objectives and purpose of the AI system and the technical requirements to design, develop and deploy such a system, including data protection, security and quality. This also comprises the definition of the expected AI system outcome, the level of control and end users' qualifications. The objectives of the AI system encompass a preliminary analysis of the data needs as well as an ethical assessment to decide whether ethical committee approval is needed.

2. Data gathering and processing. This phase involves four principal steps: (2.i) access, analysis and assessment of the raw data; (2.ii) data collection process; (2.iii) data preparation and (2.iv) data transformation. During the data collection the assets, typically code and metadata assets, are posted to the software repository, which, in turn, triggers the continuous integration process. Also, all relevant project assets (data, scripts, notebooks, flows) are copied to a build system

The selection and preparation of the data sets, including training, validation and test, plays a crucial role in the development of AI systems and requires appropriate data governance and management practices linked also to the data transformation processes (feature selection, construction and processing). Researchers and developers of AI-based solutions might request to have access to these datasets (Horgan et al, 2019, Rowley et al, 2019).

3. Data modelling. This phase comprises the final model selection and training, including the model validation using the proper datasets (validation dataset) and metrics about the performance of the AI system. In this step, cross-validation techniques are essential to estimate the performance and/or accuracy of the ML models (Xu and Goodacre, 2018). Ideally, the data used for the models should be findable, accessible, interoperable, and reusable, as well as be stored in a widely accepted way, containing adequate quantities and variety of information, in order to facilitate its use and search. A good training of the algorithms from the beginning of its design and development process, with datasets coming from a wide spectrum of patients (e.g., from different Member States or foreign countries), guaranteeing accuracy of the model and of the provided outcomes (Shaw et al, 2019; Lai et al, 2020).

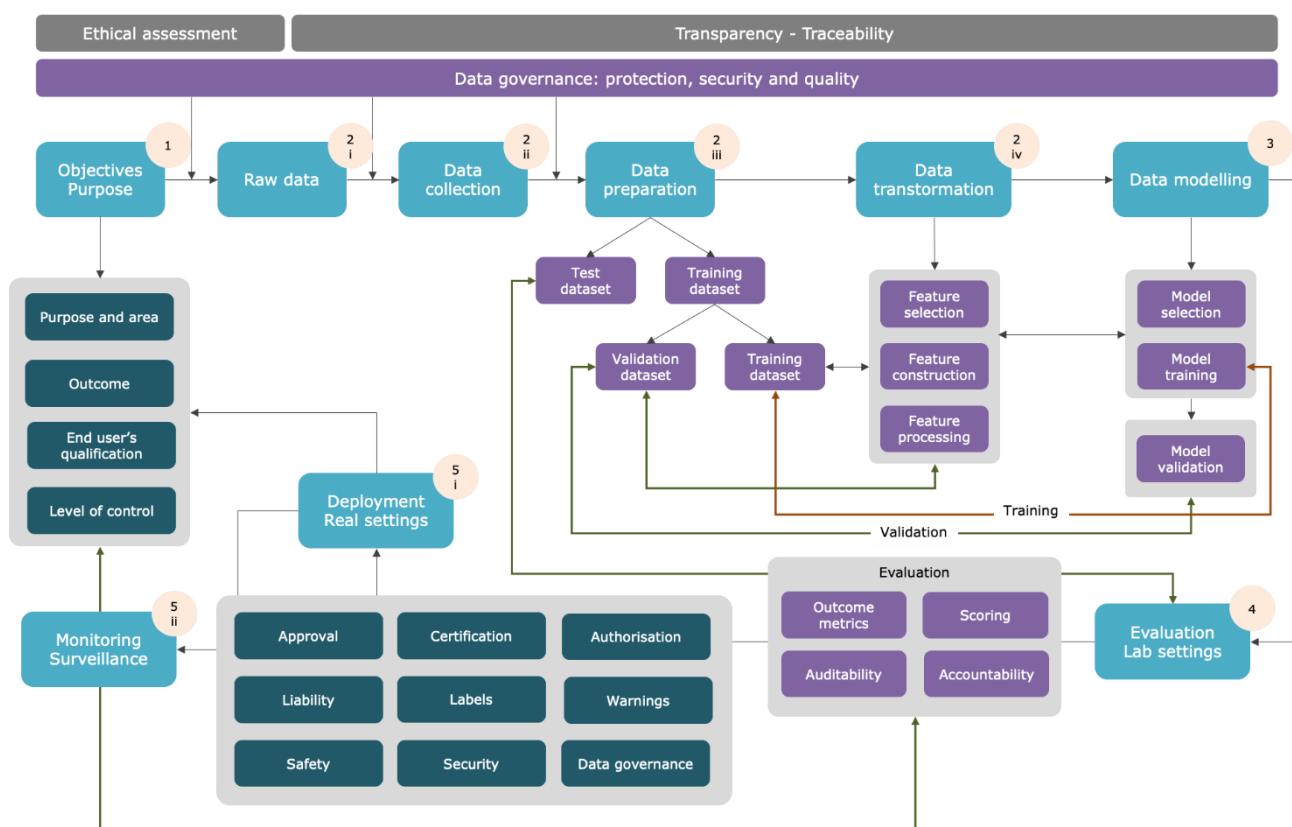
4. Evaluation (lab settings). Within this phase, the verification and validation of the models using the Test data set should be conducted. AI system, aiming to be implemented in real-world settings, should undergo rigorous validation demonstrating robustness impervious to variations in equipment and imaging protocols. (Tang et al, 2018). Critical assessment of AI solutions should be based on widely recognized principles of evidence-based medicine, including the reporting of the outcomes and the results of the clinical evaluation process. In this sense, there are existing consensus statements for the reporting of clinical evaluations results depending on the specific use case and purpose of the AI systems. For example, AI tools developed for diagnostic purposes should follow the STARD (Standards for Reporting Diagnostic Accuracy) principles. Similarly, studies reporting predictive models should be compliant with the TRIPOD (Transparent Reporting of a multivariable prediction model for Individual Prognosis or Diagnosis) statement (Tang et al, 2018). On top of that, prospective clinical evaluation is essential to ensure that AI systems are safe and effective, using clinically applicable performance metrics that go beyond measures of technical accuracy to include how AI affects the quality of care, the variability of healthcare professionals, the efficiency and productivity of clinical practice and, most importantly, patient outcomes. (Kelly et al, 2019).

5. Deployment, monitoring and surveillance. This phase is related to the deployment of the AI models in real settings, monitoring truthfulness, accuracy and long-term improvement and re-calibration of the implemented models and related outcomes through surveillance studies and activities. After the model passes the evaluation (phase 4), the integration process begins deploying the model to the production system at scale (5i) and with the relevant monitoring and surveillance measures (5.ii) to be implemented (Desouza et al, 2020).

The deployment strategies for AI systems in healthcare are currently *ad hoc* for most applications which means configuring an analytical asset for integration with other applications to serve the production workload at scale. The steps that could be followed for the implementation of AI systems, and specifically in health, are not standardized so there is a lack of defined rules and best practices leads to provisional solutions that may be suboptimal (Drysdale et al, 2020). Considering the available evidence, we can contemplate the five phases described above as the main steps for this process. Considering the above, implementation is complex, and many issues need to be addressed before, during, and after the implementation of an AI in the healthcare system (see section 3.1.5).

The following figure sketches all the steps, including relevant elements that will be further explore in this study.

Figure 5. AI system phases in health



Source: Authors' elaboration

3.1.4 AI performance and economic impact

Nowadays, there are no common, reliable and valid approaches to perform benchmarking or evaluation analysis of the different aspects related to AI performance. Furthermore, the existing benchmarks are not suitable for measuring specific aspects of AI systems such as the training

and learning process, so there is a need to establish clear testing and evaluation processes (Gómez-González et al, 2020). In this sense, two relevant main questions should be addressed through benchmark and evaluation: how ready countries and / or organisations (e.g., healthcare system) are to earn the benefits of AI and the evaluation and performance of the AI quality, accuracy, and capabilities (Tinholt et al, 2017).

Benchmarking of AI is an important issue to address the progress of AI research and its use in real-life healthcare scenarios (Gerke et al, 2020), indeed as indicated in the previous section and illustrated in Figure 5, this process is the last one before moving forward to the real settings. Robust peer-reviewed evaluation, performance metrics that capture real clinical applicability, regulations that balances innovation and potential harm of AI-based systems in healthcare, are required to ensure that patients are not exposed to dangerous situations produced by AI systems (Kelly et al, 2020).

Researchers and developers use metrics to **evaluate the models** that sometimes do not reflect their true performance, due to the inherent adaptations of these algorithms over time. AI-based systems interpretability of the algorithms could reach a level of complexity that makes difficult for humans to understand and interpret algorithms outcomes and decisions (Diebolt et al, 2018). For this reason, AI-based systems require to perform testing and evaluation processes in each new context before using them in patient's care (Carter et al, 2020).

Table 20 reports the survey results inquiring the availability of rules involving a quality benchmark or criteria for AI-based systems in healthcare. As gets visible, a vast majority of countries does not have rules involving a quality benchmark or criteria for AI-based systems in healthcare.

Table 20. Rules involving a quality benchmark or criteria for AI-based systems in healthcare

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	No
Czechia	Yes	Netherlands	No
Denmark	Yes	Poland	No
Estonia	No	Portugal	No
Finland	No	Romania	No
France	Yes	Slovakia	No
Germany	Yes	Slovenia	No
Greece	No	Spain	No
Hungary	No	Sweden	No
Ireland	No		

Source: Author's elaboration

Czechia is involved in global activities focusing on testing and evaluation of data quality and validation and performance of AI applications in healthcare which is an example of data governance structures for AI. The Danish Quality Model (DDKM) is the national and cross-cutting quality development system for publicly funded healthcare services in Denmark. DDKM is an accreditation system in which the participating private hospitals, pharmacies, practitioners and municipalities are assessed every three years with a view to obtaining accreditation¹⁰⁵, AI-based systems could be included under this framework. France does have a rule/regulation involving quality benchmark for digital healthcare and services, including AI systems among other services. This rule is compliance with Provisions of Certification on Hosting Personal Health Data, Legal and Regulatory Requirements for Data Sharing and Personal Data Processing, health data dematerialisation and assistance with drug prescriptions¹⁰⁶. Germany has identified the standardizations needs, including quality assessment of AI-based systems.¹⁰⁷

According to a study with data from over 3000 **model performance results**, the most frequently used metric is "accuracy", followed by "precision" and "F-measure" (Blagec et al, 2020). Based on the model implemented, there are different metrics to assess, for instance, to evaluate classifiers. **Accuracy** is used to assess the proximity of measurement results to the true value. **Precision** assesses the degree to which repeated (or reproducible) measurements under unchanged conditions show the same results. **Recall/Sensitivity** measures the fraction of relevant instances that were retrieved. **Precision-Recall (PR)** curves are frequently used to display these metrics for various thresholds. **F-measure**, also known as F1 score, is a harmonic average of the precision and recall. However, **Matthews Correlation Coefficient (MCC)** has been recently introduced as a symmetric measure of the quality of binary classifications. When considering survival methods, the most employed metrics are the **Area Under the Receiver Operating Characteristic (ROC) Curve (AUC)**. A ROC curve is a graph showing the performance of a classification model at all classification thresholds, where AUC – and its 95% confident interval - measures the overall model performance of a classifier, and **p-value** measures the statistical significance of the study variables. The following table summarises the most used metrics while dealing with AI modelling (Handelman et al, 2019).

Table 21. Common metrics used in evaluation of AI algorithms

Outcome metrics	Meaning
Confusion matrix	True Positive (TP): outcomes from a classifier predicted as positive being positive. True Negative (TN): outcomes from a classifier predicted as negative being negative. False Positive (FP): outcomes from a classifier predicted as positive being negative. False Negative (FN): outcomes from a classifier predicted as negative being positive.
Precision	$\text{Precision} = \text{TP}/(\text{TP}+\text{FP})$ Fraction of positive instances out of the total predicted positive instances. Also known as positive predictive value.
Recall/Sensitivity	$\text{Recall} = \text{TP}/(\text{TP}+\text{FN})$ Fraction of positive instances out of the total actual positive instances. Recall should be as highest as possible, but with a compromise with precision. Also known as True Positive Rate (TPR).
Accuracy	$\text{Accuracy} = (\text{TP}+\text{TN})/(\text{TP}+\text{FP}+\text{FN}+\text{TN})$

¹⁰⁵ Danish Institute for Quality and Accreditation in Healthcare <https://www.ikas.dk/den-danske-kvalitetsmodel/ddkm-in-english/introduction-to-ddkm/>

¹⁰⁶ National Digital Health Agency (ANS) eHealth label (Levels 1 and 2), 2016

¹⁰⁷ German Standardization Roadmap on Artificial Intelligence Section 4.7 AI in medicine <https://www.din.de/resource/blob/772610/e96c34dd6b12900ea75b460538805349/normungsroadmap-en-data.pdf>

Outcome metrics	Meaning
	Proximity of measurement results to the true value. Good accuracy is the one close to 1.
Specificity	Specificity = $TN/(TN+FP)$ Ratio of success from all the positive cases classified. Also known as true negative rate and "1 - Specificity" is known as False Positive Rate (FPR)
F1 score	$F1\ Score = 2*(Recall * Precision) / (Recall + Precision)$ Harmonic average of the precision and recall. This validation score is useful in the presence of class imbalance because it takes care of false classification rates, therefore a good choice for comparing different models predicting the same. F1 score reaches its best value at 1 and the worst score at 0.
Matthews Correlation Coefficient (MCC)	$MCC = (TP * TN) - (FP * FN)/\sqrt{[(TP+FP)*(TP+FN)*(TN+FP)*(TN+FN)]}$ MCC is symmetric and considers all four values from the confusion matrix. It ranges from -1 (classifier always misclassifies) to 1 (perfect classifier).
AUC	It is the measure of the ability of a classifier to distinguish between classes and is used as a summary of the ROC curve. It plots the FPR (1 – Specificity) versus TPR.
Exp HR (L-U)	Hazard ratios are ratio of death probabilities. Log of HR, is the estimated HR.
Standard error (coef.)	Standard deviation from the sample distribution or mean error.
z-score	The typified units show the number of standard deviations in which a given value is above or below the average.

Sources: Authors' elaboration

Additionally, other metrics are explicitly used for NLP algorithms: the BLEU score – for summarising and text generation; the ROUGE metrics – for video captioning and summarising; and the METEOR – for question-answering (Blagec et al, 2020). Specifically, the BLEU (Bilingual Evaluation Understudy) score measures precision, meaning how much the words (also named as n-grams) in the machine generated summaries appeared in the human reference summaries. The ROUGE (Recall Oriented Understudy for Gisting Evaluation) score measures recall, meaning how much the words (n-grams) in the human reference summaries appeared in the machine generated summaries. Although these scores are complementing, as is often the case in precision versus recall, they have limitations because they focus only on instances predicted as positive by a classifier or on true positives (accurate predictions). Finally, the METEOR (Metric for Evaluation for Translation with Explicit Ordering) score is a metric for machine translation evaluation, and it asserts to have better correlation with human judgement, for example in question-answering processes (Blagec et al, 2020; Ethayarajh et al, 2020).

A critical assessment of AI solutions used in healthcare should be based on the principles of evidence-based medicine, including specific use cases and metrics defined by clinicians, going beyond technical performance and analyse AI's value proposition in real-world care contexts (Johner, 2019). The evaluation process of AI-based systems has to evolve to a "versioning" model so inherent changes of the algorithms and models, as well as updates performed by the developers, can be considered and evaluated appropriately (Tang et al, 2018; Diebolt et al, 2018; Alami et al, 2020; Recht et al, 2020). The Health Technology Assessment (HTA) methodology could serve as a base to build this evaluation approach (Odone et al, 2018), together with a mechanism to ensure the quality of the data used to train and validate the algorithms, for example by sharing the datasets with other healthcare entities (see Lot 3) with the purpose of evaluation and validation (Price, 2019). van Leeuwen et al (2021) proposed a hierarchical model of efficacy to assess the contribution of AI systems going from technical efficacy (Level 1) to Societal efficacy (Level 6):

Table 22. Hierarchical model of efficacy to assess the contribution of AI systems

Level	Explanation	Typical measures
Level 1t	Technical efficacy. AI system demonstrates the technical feasibility of the software	Reproducibility, inter-software agreement, error rate
Level 1c	Potential clinical efficacy. AI system demonstrates the feasibility of the software to be clinically applied	Correlation to alternative methods, potential predictive value, biomarker studies
Level 2	Diagnostic accuracy efficacy. AI system demonstrates the stand-alone performance of the software	Standalone sensitivity, specificity, area under the ROC curve, or Dice score
Level 3	Diagnostic thinking efficacy. AI system demonstrates the added value to the diagnosis	Radiologist performance with/without AI, change in radiological judgement
Level 4	Therapeutic efficacy. AI system demonstrates the impact of the software on the patient management decisions	Effect on treatment or follow-up examinations
Level 5	Patient outcome efficacy. AI system demonstrates the impact of the software on patient outcomes	Effect on quality of life, morbidity, or survival
Level 6	Societal efficacy. AI system demonstrates the impact of the software on society by performing an economic analysis	Effect on costs and quality-adjusted life years, incremental costs per quality-adjusted life year

Sources: Based on van Leeuwen et al (2021)

Another aspect to be considered within a critical assessment of AI-based solutions in healthcare is the management and assessment of risks that include **accountability, reporting** (e.g., progress and post-implementation review reports) and **auditability** (Baig et al, 2020; Gerke et al, 2020; EIT Health Consultative Group, 2020). In this sense, the European regulatory regime adopts a **risk-based approach** when regulating medical devices. This risk-based approach is also proposed to regulate AI systems in AIA. Requirement's elicitation and risk analysis are processes included in the GDPR (Article 35) through the performance of a data protection impact assessment (Ho et al, 2019; Martinez, 2019). The performance of a risk assessment is the responsibility of the manufacturers and developers of AI-based solutions or a body assigned by authorities of EU Member States (Ho et al, 2019). In the same way, in the US, the FDA adopted a risk-based approach applied to the overall life cycle (ISO 14971) (Ho et al, 2019; Alami et al, 2020).

The difference between the US approach and the EU approach is the addition of a "Clinical Evaluation Report" and the requirement of additional clinical evaluation for class IIa and class IIb devices (medium to high-risk devices) in Europe (Angehrn et al, 2020), following the STARD (Standards for Reporting Diagnostic Accuracy) and TRIPOD (Transparent Reporting of a multivariable prediction model for Individual Prognosis or Diagnosis) reporting standards. STARD "*provides a list of essential items for reporting in diagnostic accuracy studies to improve the completeness and transparency of these studies*", whereas TRIPOD "*emphasizes the transparent reporting of study settings, outcome follow-up intervals, or precise definitions of how outcomes were defined and measured, and study design elements*" (Tang et al, 2018).

International regulatory bodies need to implement guidelines and support local organisations towards the adoption of appropriate processes to regulate software that is categorised as medical devices (SaMD) (Reddy et al, 2020) but also AI systems that might not be covered by the MDR. Regulatory agencies, in cooperation with healthcare organisations, have to support the

harmonisation of evaluation and certification practices by establishing normative standards and evaluation guidelines (e.g., Ethical Guidelines for Trustworthy AI), as well as an evaluation body for AI algorithms in healthcare (Diebolt et al, 2018; Esmaeilzadeh, 2020; Gómez-González et al, 2020; Reddy et al, 2020). Some initiatives have been implemented during recent years, but still there is a need for a European evaluation body for AI algorithms in healthcare (Diebolt et al, 2018).

In the US, the FDA has proposed Guidance on SaMD, including clinical evaluation and software pre-certification program for market approval (Reddy et a, 2020; Gerke et al, 2020). In addition, the FDA is currently developing a framework for the regulation of AI systems that “self-update” based on new datasets used, benchmarking the model, and ensuring clinical meaningful outcomes considering a total product lifecycle-based regulatory process (Asan et al, 2020). This approach will ensure the safety and effectiveness of the SaMD while allowing modifications of the AI algorithms coming from real-world learning and adaptation. However, currently there is a lack of clarity of the processes and methods to be applied for the approval of these type of AI-based medical devices and algorithms (Benjamins et al, 2020). The AIA and its application in the health domain could bring clarity to the current scenario (see section 3.2.4). Several experts consulted during the stakeholders’ engagement declared that the relationship between MDR and AIA might require further clarifications. It is worth mentioning the study conducted by van Leeuwen et al. (2021): an analysis of 100 commercially available products and their scientific evidence shows that *“even though the commercial supply of AI software in radiology already holds 100 CE-marked products, we conclude that the sector is still in its infancy. For 64/100 products, peer-reviewed evidence on its efficacy is lacking. Only 18/ 100 AI products have demonstrated (potential) clinical impact”* (van Leeuwen et al., 2021)

Link to the clinical impact, assessing the economic impact of AI in healthcare plays a crucial role for all healthcare stakeholders and therefore needs to be considered in detail. Comparison between AI and clinicians regarding diagnostic performance showed that AI can deliver equal results, for example in fields related to image recognition (Wolff et al, 2020). This can also, among others, support a reallocation of medical capacities, as pointed out by the health experts interviewed. In addition, AI can also enable a change from a generalized treatment to a more personalized one. Studies on the implementation and use of Computerized Clinical Decision Systems including AI revealed a positive economic impact on providers and resulted on saving an estimated US \$92,000 per year. Even these direct applications have real potential, adoption in professionals and providers day-to-day operations remains comparatively low. The reasons for this are multiple and include social, ethical, legal or technological barriers. However, the most powerful barrier remains economic. Healthcare providers see upfront and ongoing maintenance costs as key barriers to adoption and often question the overall cost effectiveness of these solutions (von Wendel et al, 2020). This could also be linked to further increasing costs if very strict liability is imposed. As shown in future sections, it is important to understand the market value of health data and the economic benefits it could bring to both Member States and patients.

From the point of view of the medical professionals and industry experts interviewed, the implementation of AI systems implies an increase in costs. However, this economic impact makes sense if it has been done a projection study wherein the medium or long term is going to translate into reducing, for example, medical tasks and that in some way will be a return, which will have a huge positive impact. Therefore, there is a need to conduct cost-effectiveness studies of the interventions using AI systems in health. To facilitate and reinforce investment in AI, and to maximize its impact in both the public and the private sectors, joint efforts between the Commission, Member States and the private sector are considered necessary. Only if both the Commission and Member States direct their investments in the same direction through joint

programming and leverage significant private investments, will Europe have an impact and establish its strategic autonomy in AI. To do this, the European Commission proposes public and private investments in AI must be scaled up to reach the target of EUR 20 billion per year over the next decade. And to contribute to this, under the Digital Europe Program, the Commission envisages making available around EUR 1.5 billion to establish world-leading testing and experimentation sites for AI-powered products and services throughout Europe under the next programming period 2021-2027.

Box 25. Implementation of AI systems

From the point of view of the medical professionals and industry experts interviewed, the implementation of AI systems implies an increase in costs. However, this economic impact makes sense if it has been done a projection study wherein the medium or long term is going to translate into reducing, for example, medical tasks and that in some way will be a return, which will have a huge positive impact. Therefore, there is a need to conduct cost-effectiveness studies of the interventions using AI systems in health. To facilitate and reinforce investment in AI, and to maximize its impact in both the public and the private sectors, joint efforts between the Commission, Member States and the private sector are considered necessary. Only if both the Commission and Member States direct their investments in the same direction through joint programming and leverage significant private investments, will Europe have an impact and establish its strategic autonomy in AI. To do this, the European Commission proposes public and private investments in AI must be scaled up to reach the target of EUR 20 billion per year over the next decade. And to contribute to this, under the Digital Europe Program, the Commission envisages making available around EUR 1.5 billion to establish world-leading testing and experimentation sites for AI-powered products and services throughout Europe under the next programming period 2021-2027.

Source: Authors' elaboration based on in-depth interviews

Many countries are investing significant amounts of money in AI research and development, with more than \$20 billion invested by the United States, China, and the United Kingdom alone in 2016 (Kelly et al, 2019; Shinners et al, 2020). The global market for AI in healthcare is projected to grow at an annual growth rate of 43.5% beginning in 2018, reaching a valuation of US \$ 27.6 billion by 2025 (Barbour et al, 2019). Additionally, Accenture estimates that "key applications of AI for clinical health" can generate annual savings of \$150 billion for the US healthcare economy by 2026 (Stanfill et al, 2019).

3.1.5 Challenges of AI use in healthcare

The healthcare sector is increasingly incorporating emerging digital solutions to improve clinical, processes and organizational outcomes. Among them, **AI brings new opportunities** in the management of diseases and clinical pathways, disease prevention, care delivery and patient empowerment. The implications of incorporating and scaling-up AI-based solutions in the healthcare system have been debated during the recent years (Fernández et al, 2020). This debate covers questions related to AI potential impact on healthcare professionals and healthcare specialities, the risks and ethical concerns related to its implementation, the role in public and private healthcare systems, impact on the efficiency of care delivery and patient experience, and better care outcomes (Fernández et al, 2020). AI methods are achieving unprecedented levels of performance when learning to solve increasingly complex computational tasks, making them pivotal for the future development of the human society (Arrieta et al., 2020). Nevertheless, there remain a number of issues that create uncertainty and render clarification.

A major challenge in deploying AI is the **ethical challenge**. Data security and patient privacy are of utmost importance when considering AI implementation. Patients may not be aware that their data is used, shared, or sold for AI system development (Rai et al, 2020). This problem was further amplified because most AI systems are not transparent about their training samples and the demographic distribution of training data is often not reported. The lack of representativeness of the population is a path towards bias and unintended consequences for the implemented models (Hu et al, 2020). On top of that, according to the conclusions from expert consultation, lack of trust is a barrier on data sharing and deployment of AI in hospital which is very much linked also with cultures and countries so collaboration among states is fundamental to make the deployment of AI a reality. Also, it is essential to work on how to engage these systems in the dynamics of the day-to-day clinical flow. For this, while it is being implemented, there is a clear need for raising awareness and train the medical environment.

The role of AI in the healthcare domain is related to its implication in each step of **the patient journey**, from the prevention phase where personal health and lifestyle choices are monitored (e.g., through wearables and personalised applications), to clinical diagnosis (e.g., supported by virtual assistants, imaging or lab AI systems) and care and treatment provision (e.g., surgical robots, personalised applications, remote monitoring) (Biundo et al, 2020). AI technologies can empower patients, for example by helping them monitor their health to make healthier decisions, and by supporting doctors in the diagnosis and treatment of their health conditions.

Furthermore, AI-based solutions allow healthcare professionals to have access to a rich pool of knowledge that may lead to accurate diagnoses and practices (Ho et al., 2019; Lai et al, 2020; Biundo et al, 2020). These solutions **can offer many benefits** such as improve medical provision and care delivery leading to the reduction of errors and lower costs (e.g., early diagnosis, reduce unnecessary hospital visits and adverse events, selection of targeted treatments that improve patient's outcomes); improve the efficiency and effectiveness of healthcare services by predicting hospital bed or ER availability, prioritize discharging patients and better anticipate patient demand through patient forecasting; lessen the burden on medical professionals (e.g. improving day-to-day healthcare practices); and improve medical research providing the possibility to answer complex scientific questions through the use of existing health data (Diebolt et al, 2018; Rowley et al, 2019; Horgan et al, 2019, Fernández et al, 2020).

Although AI provides multiple benefits and has a promising potential in the healthcare sector, **there are still barriers to be addressed, such as: legal implications, technical interoperability with existing healthcare systems, and data sharing**. If these barriers are correctly removed, benefits to personalized, preventive, participative, precision and population medicine models can become a reality, improving patient's outcomes and the efficiency of the health sector.

Key challenges to incorporate AI technology into healthcare include those intrinsic to the AI systems techniques (e.g., interoperability of the data set, data protection, data quality), barriers and difficulties to implement and adopt AI systems in the healthcare sector (e.g., digitalisation adoption, cost of AI technologies, skills and training, shift from care to prevention) and sociocultural changes (e.g., policies changes, norms, religion, governance, and market exchange). Data challenges are further addressed in Lot 3. Furthermore, one of the most debated challenges of AI in healthcare is the **lack of a regulatory framework** that balances innovation with the possibility of system failure to ensure that patients are not exposed to dangerous situations. The AIA and DGA (including the forthcoming EHDS) proposed by the EC could be considered as a first step to cover this gap. They will provide a horizontal framework and foundations on the development and deployment of AI systems. However, how these requirements should be interpreted and applied to AI in healthcare requires further development

in addressing the challenges in healthcare that are identified in this study (see section 3.2.4). During the consultation activities conducting in this study, we were not able to identify any Member States adopting specific rules for the organisation and provision of healthcare when AI is involved.

Table 23. Rules adopted for the organisation and provision of healthcare when AI is involved

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	Yes ¹⁰⁸	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	No
Czechia	No	Netherlands	No
Denmark	No	Poland	No
Estonia	No	Portugal	No
Finland	No	Romania	No
France	No	Slovakia	Yes ¹⁰⁹
Germany	No	Slovenia	No
Greece	No	Spain	Yes ¹¹⁰
Hungary	No	Sweden	No
Ireland	No		

Source: Authors' elaboration

All these challenges can be categorized and explored in four categories, that will be discussed below: clinical, technological, ethical-regulatory, and economic.

Clinical factors. The incorporation of AI in healthcare raises challenges that if not covered will prevent effective performance and adoption into **clinical practice** such as: (1) the need of robust, coherent and accurate **clinical evaluations** to ensure the safety of AI systems and precision of their clinical outcomes; (2) the difficulty to distinguish the **added value** of AI decisions from current preventive and/or therapeutic strategies; and (3) the **lack of trust** in the accuracy of AI decisions when used in daily clinical practices (Alami et al, 2020). In this sense, the European Commission AI High Level Expert Group (AI HLEG) - appointed by the EC in June 2018 - published the "Ethics Guidelines for trustworthy AI" (AI HLEG, 2019). The Guidelines promote the slogan "Trusted AI" and contain seven principles that AI healthcare systems must meet to be trustworthy. These principles are: (1) human agency and oversight, (2) technical robustness and security, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and equity, (6) environmental and social well-being, and (7) responsibility (Gerke et al, 2020). If these principles are adopted, the utilization of AI in the

¹⁰⁸ The general rules for liability in tort under the Bulgarian Obligations and Contracts Act (SG 275/1950, as amended) apply.

¹⁰⁹ Slovak law does not distinguish between physicians' liability in case of provision of health care using telemedicine and liability in case of provision standard health care. The Action Plan on the Digital Transformation for 2019-2022 intends to establish a Permanent Commission on the Ethics and Regulation of AI, which should deal with the issues related to liability for damage.

¹¹⁰ Could be regulated by the Law 41/2002, of November 14, regulating basic patient autonomy and rights and obligations regarding information and clinical documentation.

medical practice will be consequently benefited, and eventually boosting the outcomes of the healthcare sector, as it is already happening in other industrial and societal domains.

Technological factors. From a technological standpoint, AI algorithms implemented in the healthcare domain have the potential to suffer from weaknesses, including bias, lack of explainability, interpretability, and transferability. The healthcare data could be biased against disadvantaged groups because sometimes these groups are under-represented while collecting clinical data in daily medical practice and conducting clinical studies defined by healthcare professionals (Hacker, 2018; Carter et al, 2020). Considering that healthcare delivery already varies by ethnicity, it is possible that some ethical biases are inadvertently incorporated into medical algorithms (Martínez, 2019; Carter et al, 2020). Consequently, **AI may reinforce discrimination bias** unless explicit human choices are made, because it may bring to discriminatory human decisions (Hacker, 2018; Martínez, 2019; Zuiderveen Borgesius, 2020; Carter et al, 2020). **Bias in healthcare outcomes** is a problem presented in ML systems used in healthcare, arising from bias in the health-related data used for the training and validation of the algorithms or algorithm design choices (Schönberger, 2019; Zuiderveen Borgesius, 2020). In addition, ML models can also incorporate implicit selection biases from the demographics of the population used for its training, which may not be representative of the target population in which it will be applied (Ho et al, 2019). ML classifiers usually improve with the volume of data used, nevertheless there is naturally proportionally less data available about minorities (Schönberger, 2019). In the healthcare domain it becomes essential to minimize these potential risks of bias, so it is technically and ethically necessary to design AI systems that help compensate for human biases and lead to fairer and accurate healthcare outcomes that provide realistic information covering all possible options and considering all the differences of human beings. This approach will lead to avoid errors in healthcare provision arising from inappropriate AI models and health-related datasets (Horgan et al, 2019; Reddy et al, 2020).

Other technological challenge faced by AI systems in healthcare is related to the necessity of understand the AI model reasoning and its outcomes, known as explainable and interpretable AI. AI algorithms are often characterized as "**black boxes**", because it can generate complex models that are difficult (if not impossible) to interpret. However, clinical professionals not seeing black boxes in medicine can work without human interventions. A solution proposed during stakeholders' consultation with experts is using "collaborative intelligence" which means combining AI and the human intelligence. The explainability and interpretability of the AI models is paramount to solve this problem in the healthcare decision-making process (e.g., diagnosis, prognosis, prediction) (Vellido, 2019). When used in real clinical practice, the black box problem is characterised by the lack of understanding of how the algorithms arrive at clinical decisions, even for the developers of the algorithms (Zuiderveen Borgesius, 2020; Carter et al, 2020). Finally, the last technological challenge faced by AI systems in healthcare is **transferability**, which contemplates that an algorithm trained and tested in a particular environment and dataset, could not be applied in other environments and datasets (Carter et al, 2020).

Ethical and regulatory factors. As regard of **ethical-regulatory challenges**, a fundamental component to achieve a safe and effective deployment of AI systems in health is considering the development of regulatory and ethical frameworks. This poses a unique challenge given that, although ethics is an under-explored aspect of AI in health, it involves a fundamental concern in healthcare daily practices. Therefore, it becomes important to create a clear roadmap for the ethical use of AI in medicine considering that the application of AI in areas of social relevance should also aspire to be fair (Vellido, 2019). Initiatives such as the European Ethics Group briefly

refer to "responsibility" as an "obligation to account". (Schönberger, 2019). The Dutch Ministry of Health already has developed a method to guide ethical use of AI in health¹¹¹.

On the other hand, developing a **modern regulatory framework** to ensure that AI-based devices are safe and effective, will bring confidence to physicians, healthcare systems and policy makers (Sun et al, 2018). Current regulations on medical devices include software within their scope, differentiating between software independent or incorporated into an existing device, and based on the intended purpose of the solution. Standards that cover the application of traditional Software as a Medical Device (SaMD) have been developed in recent years. However, healthcare AI-based software and systems introduce a new set of challenges that had not been considered before within the SaMD such as the one related to liability and accountability coming from (Rowley et al, 2019):

- the level of autonomy introduced by AI-based technologies;
- the ability of continuous learning, where systems can change their outcomes over time in response to new data; and
- the ability to explain and understand how a result has been achieved.

These issues cause regulatory challenges in particular with view to liability questions in case of injuries caused by AI systems. The use of autonomous self-learning systems complicates the application of existing tort law when trying to resolve claims of malpractice. At the same time, legal challenges are considered one of the potential barriers to the adoption of AI in European healthcare (Ordish, 2018).

Economic factors. Finally, economic challenges include obstacles related to profitability and economic sustainability that inhibit the adoption of AI in healthcare (e.g., high treatment costs for patients and non-profit for hospitals), including the need for large and continuous investments in performance testing, data quality testing and software, infrastructure and equipment upgrades, human expertise and training. In addition, new financing mechanisms, adequate remuneration or reimbursement models and insurance models are needed to prevent extra costs for patients, doctors, organizations, and health systems (Sun et al, 2018; Wolff et al, 2020).

Social factors. There is a perceived societal misunderstanding of the capabilities of AI technologies in the public healthcare sector, that leads to high expectations in society and difficulties in the acceptance of AI technologies applied to the healthcare sector (Sun et al, 2018).

Political, legal and policy factors. Challenges under this category are related to political considerations of possible national security threats coming from the use of sensitive data between countries, lack of market-wide policy regulations and legal regulations addressing accountability of AI-based systems used in healthcare decision-making (Sun et al, 2018).

Organizational and managerial factors include the following: issues at a strategy level, such as the lack of strategy plans for AI development; issues at a management level, such as organizational resistance to data sharing; and issues at a human resource (HR) level, such as the lack of skilled workforce and the perceived threats of workforce replacement (Sun et al, 2018).

The healthcare community needs to be trained in understanding and knowing how to address these challenges, as they represent the mediator between AI systems and its end-use.

¹¹¹ Ethische kaders | Wegwijzer AI in de zorg | Data voor gezondheid <https://www.datavoorgezondheid.nl/wegwijzer-ai-in-de-zorg/ethische-kaders-ai-in-de-zorg>

Additionally, the establishment of standards and guidelines will allow that the dyad of physician and AI systems working together produce the greatest potential to improve clinical decision-making and patient health outcomes (Paranjape et al, 2020). In addition, it is worth mentioning that certain medical specialties, particularly those related to image, data analysis and interpretation (e.g., radiology, pathology, dermatology, epidemiology, public health and the different branches of surgery) will experience in the next years profound transformations (some of which have already started) due to the adoption of new tools with expanding capabilities and increasing autonomy (Gómez-González, E et al, 2020).

3.2 Regulatory landscape and gaps

3.2.1 Current EU framework

Despite the lack of specific regulations in the area of AI in health, several entities (EU Parliament, UK House of Commons, AI expert groups, EC, etc.) have been working on **initiatives and new strategies to address the challenges of increased usage of AI in different domains**.

Most EU countries have put forward national AI strategies, while the industry itself has been active to develop own AI principles or best practices (Cath, 2018). In 2016, the European Parliament and the UK House of Commons delivered reports providing guidelines and information on how to prepare society for the widespread use of AI. Although these reports gave an initial path towards the implementation of AI in different sectors of society, they did not deliver an explicit vision of the role of AI in mature information societies (Cath et al, 2018). The following table summarizes the EU regulations by type of issue addressed:

Table 24. EU regulations by type of issue addressed

Issue	Rules
Safety, technical robustness and accountability	<ul style="list-style-type: none"> • Art. 22 GDPR access rights in case of 'automated decision-making' • Radio Equipment Directive (RED) • Machinery Directives¹¹² • Medical Device Regulation <ul style="list-style-type: none"> ◦ Article 1(2) of Directive 93/42/EEC replaced by MDR on 26 May 2020 ◦ MDR (EU) 2017/745 and 2017/746, medical device also as in vitro diagnostic medical device qualification ◦ Art. 123(1) MDR ◦ Art. 122 MDR (90/385/EEC AIMD), active implantable medical devices ◦ Recital 40 and Art. 2(43) MDR, CE marking ◦ Art. 52 and Annexes IX_XI MDR, CE marking ◦ MDR, Annex I, Chapter II, 17.1 - General Safety and Performance requirements ◦ MDR Annex I, Chapter II, 17.2 - General Safety and Performance requirements ◦ MDR, Annex II, 6.1 - Technical requirements • ISO/IEEE 11073-20702, Service-oriented Device Connectivity (SDC) for interconnection of medical devices • In Vitro Diagnostic medical devices Regulation (IVDR) <ul style="list-style-type: none"> ◦ Art. 113(1) IVDR, in vitro diagnostic medical devices AI in Healthcare ◦ Art. 113(2) and (3) IVDR ◦ Art. 112 of the IVDR ◦ IVDR, Annex I, Chapter II, 16.1 - General Safety and Performance requirements

¹¹² See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products COM/2021/202 final mentions software of the control system when addressing safety and reliability "a fault in the hardware or the software of the control system does not lead to hazardous situations".

Issue	Rules
	<ul style="list-style-type: none"> ○ IVDR Annex I, Chapter II, 16.2 - General Safety and Performance requirements ○ IVDR, Annex II, 6.4 - Technical documentation, specifically pre-clinical and clinical data requirements
Privacy, security and data governance	<ul style="list-style-type: none"> • GDPR 2016/679 ○ Art. 35 GDPR, data protection impact assessment ○ Directive 95/46/EC Data protection replaced by GDPR ○ Art. 29 GDPR, 'explicit' refers to 'the way' consent is given and requires an 'express statement' ○ Art. 13(1)(f), 14(1)(g), 15(1)(h), access rights in case of 'automated decision-making' ○ Article 5(1)(b), health-related data for public interest scientific research purposes 'clarify on the interpretation' ○ Art 6 (1)(a); Art 9 (2)(i)(j) ○ Art. 22, access rights in case of 'automated decision-making' • European Convention on Human Rights (1950), right to private life ○ Article 8 of the European Convention on Human Rights (ECHR) • Charter of Fundamental Rights of the European Union, private life and protection of personal data ○ Article 7 of the European Charter of Fundamental Rights • Directive (EU) 2016/1148 – cybersecurity
Transparency	<ul style="list-style-type: none"> • Art. 5 GDPR, lawfulness, transparency, guarantee of rights • Article 15. Right of access by the data subject
Diversity, non-discrimination and fairness	<ul style="list-style-type: none"> • Art. 21 of the Charter of Fundamental Rights • Directives: <ul style="list-style-type: none"> ○ Directive 2000/43/EC, the Race Equality Directive ○ Directive 2000/78/EC, the Framework Directive, guards against discrimination based on religion or belief, disability, age, or sexual orientation in employment matters. ○ (iii) Directive 2004/113/EC, the Goods and Services Directive: gender discrimination. ○ (iv) Directive 2006/54/EC, the Gender Equality Directive. • EU anti-discrimination law, Non-discrimination Law and Data Protection Law • Art. 15(1) GDPR • Art. 14 of the European Convention on Human Rights
Other issues (Robotics, Loss/harm, cross-border)	<ul style="list-style-type: none"> • Civil laws concerning Robotics (European parliament, February 2017) • Commission on Civil Law Rules on Robotics (2015/2103(INL)) • Tort law, protecting from loss or harm, resulting in legal liability for the person who commits the tortious act • 2011-24 Cross-border Healthcare Directive

Source: Author's elaboration

In the remainder we outline the most relevant regulations at EU level that govern the use of AI in health in more detail.

General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (GDPR)** was put into effect on May 25 2018 and is a major step for building trust for citizens in data privacy and security at a time when more people are entrusting their personal data with cloud services. Through the adoption of the GDPR the European Union (EU) was the first to attempt to regulate AI through data protection legislation (Bourassa Forcier et al., 2019). At the same time, the adoption of the GDPR also paved the way for meaningful reforms in privacy legislation in the US and Canada as its extra-territorial reach puts pressure on both countries to update their own legislation to secure data flows from Europe. **While AI is not explicitly mentioned in the GDPR, many provisions in**

the GDPR are relevant to AI, and some are indeed challenged by the new ways of processing personal data that are enabled by AI.

AI technologies generally require large amounts of both personal and non-personal data to function (Bourassa Forcier et al., 2019). **In health care sector specifically, AI technologies rely on personal information**, including health-related data extracted from medical files or research participants' results. This is why privacy protection is essential, especially with individuals showing substantial concerns about sharing their data in the medical and clinical context. Most importantly, in order to be compliant with the GDPR, data protection principles must be considered in the design of any new product or activity, while these principles should be consistent with the beneficial uses of AI and big data. The information requirements established by the GDPR can be met with regard to AI-based processing, even though the complexity of AI application has to be taken into account especially with regard to the provision of informed consent by data subjects.

The **GDPR covers all personal data processed** by a data processor or controller established within the Union (art. 3.1, GDPR). It also extends to personal data of any data subject in the EU, no matter the establishment of the processor in two situations: whenever this processing is related to the offering of goods or services to data subjects in the Union; and when related to the monitoring of their behaviour within the Union (art. 2.2, GDPR). This means that many foreign companies' activities may fall into the scope of the GDPR (Bourassa et al., 2019). The information made available to data subjects should enable them to understand the purpose of each AI-based processing and its limits, even without going into unnecessary technical details (European Parliament, 2020b). Hence, it prescribes sufficient **transparency for data subjects to understand how their data is being processed**. The GDPR allows for inferences based on personal data, provided that appropriate safeguards are adopted. For example, profiling is in principle prohibited, but there are ample exceptions (contract, law or consent). A number of uncertainties still exist with regards to the GDPR concerning the extent to which an individual explanation should be provided to the data subject. It is also uncertain to what extent reasonableness criteria may apply to automated decisions (European Parliament, 2020b). The proposed Artificial Intelligence Act will shed some light on the classification of AI applications presenting high risks and therefore require a preventive data protection assessment, and possibly the preventive involvement of data protection authorities when it comes to the processing of personal data.

On a horizontal level, the GDPR offers many options for **effective supervision and enforcement on fairness, transparency, individual rights and granting an individual control over their personal data**. It does not affect algorithms that do not process personal data or that impact population rights (e.g. democracy). Sometimes, AI is not based on any personal data, meaning that no data protection regulation applies in these circumstances. The criteria for defining what is personal versus non-personal data then become crucial for determining the scope of application of a data regulation. In cases of non-personal data, the Regulation (EU) 2018/1807 on the free flow of data aims at strengthening the free circulation of non-personal data and facilitating the development of a common digital market within the EU.

Medical Device Regulation (MDR)

The use of AI and ML in medical devices is an important part of the healthcare industry with the potential to improve patient care, as well as administrative processes by automating tasks and achieving faster results. Real-world applications of AI and ML in medical devices include for example imaging systems used for diagnostic information, smart electrocardiograms estimating the probability of a heart attack, and AI-assisted stethoscopes that patients can use at home

(see also section 3.1.2). The greatest benefits of AI/ML in software resides in its ability to learn from real-world use and experience, and its capability to improve its performance. The ability for AI/ML software to learn from real-world feedback (training) and improve its performance (adaptation) makes these technologies **uniquely situated among software as a medical device** (SaMD) (Celegence, 2020). Industry representatives (COCIR, 2020) considers that the very fact that AI has been present for so long in medical devices, safely and effectively, is considered a demonstration that the medical device legislation in the EU has been an adequate legislative framework for its placing on the market. . However, the EU directives and regulations (e.g. MDD, MDR), and the harmonised standards (e.g. EN IEC 62304) **do not have concrete provisions or guidelines on medical devices which incorporate AI and ML**. As it has been reported before, an analysis of 100 commercially available products and their scientific evidence shows that “*even though the commercial supply of AI software in radiology already holds 100 CE-marked products, we conclude that the sector is still in its infancy. For 64/100 products, peer-reviewed evidence on its efficacy is lacking. Only 18/ 100 AI products have demonstrated (potential) clinical impact*” (van Leeuwen et al., 2021)

The new medical devices Regulation (2017/745/ EU) (MDR) and the new in vitro diagnostic medical devices Regulation (2017/746/EU) (IVDR), entered into force in May 2017, will replace the existing medical devices Directive (93/42/EEC) (MDD), the active implantable medical devices Directive (90/385/EEC) (AIMDD) and the in vitro diagnostic medical devices Directive (98/79/EC) (IVDD). The medical devices Regulation (MDR) (2017/745/EU) will apply from 26 May 2021 and the in vitro medical device Regulation (IVDR) (2017/746/EU) will apply from 26 May 2022 – the respective Dates of Application (DoAs). The new regulations respond to the changing medical device market, with the highest number of devices being used by consumers instead of only by clinicians (PHG Foundation, 2019). These regulations were launched before the proposed AIA and DGA.

The classification of medical devices (MDs) into four classes (Class I, IIa, IIb, III) remains, but the MDR reclassifies certain devices and has a wider scope. For manufacturers, the Regulations add new requirements and reinforce existing requirements. Manufacturers have to put systems in place for risk and quality management, conduct clinical or performance evaluations, draw up technical documentation and keep all of this up to date. Manufacturers are also required to apply conformity assessment procedures to place their devices on the market. **The level of clinical evidence needed to demonstrate the conformity of a device depends on its risk class.**

The MDR introduces new classification rules, based on which manufacturers must determine the risk class of their devices. In doing so, manufacturers must consider risk classes that may differ from the class assigned under the MDD, e.g., devices may have been ‘up-classified’ from Class I to Class IIa/IIb/III. To classify a device under the MDR, the **intended purpose** of the device and its inherent risks should be taken into account. Manufacturers based in non-EU countries need to appoint an authorised representative based in an EU Member States before their device can be placed on the market. In all cases, **manufacturers should identify a person responsible for regulatory compliance**. The MDR and IVDR currently do not allow manufacturers to place AI-based devices on the market intended to change outside of the change envelope or to suggest claims, intended uses or use conditions to the device for which no conformity assessment was carried out. Changes on use conditions require an update of the technical documentation, including the clinical evaluation and a new conformity assessment to be carried out¹¹³.

¹¹³ U MDR Art. 27(3) and EU IVDR Art. 24(3)

Product Liability Directive (PLD)

The **Product Liability Directive (PLD)**¹¹⁴ is the main reference point for product liability rules under EU law in order to ensure consumer protection. PLD serves two overall functions: (1) balancing the need not to hinder socially economic activities and technological progress, with that of granting a fair allocation of the risks and costs arising thereof, through rules that ensure safe products and adequate compensation, (2) and harmonizing national rules on product liability, to ensure high level of consumer protection and fair competition among businesses across Member States, thus contributing to the establishment of the single market (European Parliament, 2020c). The PLD provides **exhaustive harmonization of liability rules regarding damages caused by defective products**, but leaves untouched non-harmonised national legislation, so that the injured party may still rely on national provisions on damages based on contractual liability, or non-contractual liability other than product-specific ones. It **establishes a technology neutral and horizontal regime** covering a very broad range of products. Although it applies equally to products with and without software, it is not always clear how the rules should be applied to software itself, since its authors had traditional movable, mass-produced and tangible products in mind when they drafted the Directive in the 1980s. As suggested in a study conducted for the European Parliament (2020c), the PLD may qualify as a general rule, covering both traditional products and new technologies which could extend to AI systems.

Other relevant acts

The European Parliament published a resolution called "**Civil Law Rules on Robotics**" (EU Parliament resolution of 16 February 2017). In this resolution, the EU Parliament addresses some of the current challenges of AI-based systems, including recommendations directly to the Artificial Intelligence in Healthcare Commission on Civil Law Rules on Robotics (2015/2103(INL)). In April 2018, a "**first mapping of liability challenges for emerging digital technologies**" was described by the Commission Staff Working Document on Liability for Emerging Digital Technologies (Gerke et al, 2020).

The recommendations from "**Civil Law Rules on Robotics**" to the EU Commission included issues related to (Cath et al, 2018):

- The creation of a "European Agency for Robotics and AI" formed by regulators and technical and ethical experts;
- Refocusing educational goals;
- The creation of clear rules for the development and deployment of AI and robotics;
- Governance of robotics and AI;
- The creation of a "guiding ethical framework for the design, production and use" of AI and robotics;
- Liability of the industry and autonomous robots when harms occur.

In recent years, the European Union has prioritised the development of AI in order to become more competitive in the field. More precisely, the ambition is for the European Union to become the world-leading region for developing and deploying cutting-edge, ethical and secure AI, promoting a human-centric approach in the global context. The process of creating an EU-wide regulatory framework started with the Declaration of Cooperation on Artificial Intelligence, which

¹¹⁴ Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member State concerning liability for defective products

was signed by 29 countries on 10 April 2018 and subsequently by Croatia in July 2018. By signing the declaration, EU Member States expressed their willingness to cooperate on a comprehensive and integrated EU approach to AI.

In December 2018 the European Union launched the Coordinated Plan on Artificial Intelligence "Made in Europe", which proposes some 70 joint actions for closer and more efficient cooperation between EU Member States and the European Commission in key areas. This plan proposes joint actions for closer and more efficient cooperation between Member States, Norway, Switzerland and the Commission in four key areas: increasing investment, making more data available, fostering talent and ensuring trust. Stronger coordination is essential for Europe to become the world-leading region for developing and deploying cutting-edge, ethical and secure AI.

The **EU is currently evaluating a product liability framework to regulate 'emerging digital technologies' including AI** (Recht et al., 2020). Furthermore, in 2020, the Commission published a report on the broader implications for, potential gaps in and orientations for, the liability and safety frameworks for artificial intelligence, the Internet of Things and robotics¹¹⁵ and in 2021 an inception impact assessment and consultation process.¹¹⁶

The **revised Coordinated Action Plan**¹¹⁷ published alongside the AIA proposal brings forward a concrete set of joint actions for the European Commission and Member States on how to create EU global leadership on trustworthy AI. It endorses an alignment of AI policies of Member States to address global challenges and remove fragmentation, including fragmentation between various EU actions as well as fragmentation between national and EU actions could slow progress in the take-up of AI and fumble the achievement of benefit. The reviewed coordinated Plan puts forward four key sets of proposals for the European Union and the Member States: (1) Set enabling conditions for AI development and uptake in the EU, (2) Make the EU the place where excellence thrives from the lab to the market, (3) ensure that AI works for people and is a force for good in society, (4) and build strategic leadership in high-impact sectors (including health under chapter 12).

The European Commission has welcomed initiatives such as the final "**Ethics Guidelines for Trustworthy Artificial Intelligence**"¹¹⁸ prepared by the High-Level Group on Artificial Intelligence published on 8 April 2019 and the "**Report on liability for Artificial Intelligence and other emerging technologies**" prepared by the Expert Group on Liability and New Technologies published in 2019. As discussed earlier in this report, some AI applications may raise new ethical and legal questions, related to liability or fairness of decision-making (HLEG, 2019). The Ethics guidelines contain seven key principles that AI systems needs to fulfil to be trustworthy (Cath, 2018; Gerke et al, 2020). These principles are:

1. Human agency and oversight.
2. Technical robustness and safety.
3. Privacy and data governance.
4. Transparency.

¹¹⁵ <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064>

¹¹⁶ Civil liability – adapting liability rules to the digital age and artificial intelligence
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en

¹¹⁷ COM(2021) 205 final

¹¹⁸ REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics COM/2020/64 final <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

5. Diversity, non-discrimination, and fairness.
6. Environmental and societal well-being.
7. Accountability.

Experts in law confirm that from the March 2020 release of the data strategy, the states have been adopted mainly guidelines like soft law tools to coordinate on the data strategy and that usually almost every European state is adopting their report on artificial intelligence which is reported. The EC Joint Research Centre (JRC) and the Directorate General for Communications Networks, Content and Technology (DG CONNECT) developed "**AI Watch**", an initiative to monitor industrial, technological and research capacity, policy initiatives in the Member States. This initiative comes up from the **Coordinated Action Plan** communicated by the European Commission in December 2018 (COM(2018) 795 final). In this plan the Commission proposed **to work with Member States on a coordinated plan on AI by the end of 2018**, with the aim to maximise the impact of investments at EU and national levels, encourage synergies and cooperation across the EU, exchange best practices and collectively define the way forward to ensure that the EU as a whole can compete globally. Member States, Norway, Switzerland and the Commission prepared the plan between June and November 2018. This plan consisted of a series of common actions to increase investments, pool data, foster talent and ensure trust, building on the European strategy with the purpose of reaching **common objectives and complementary efforts**.

As part of the European strategy, the creation of **European data spaces** aims to identify high-value data sets by Member States to make them more openly reusable. For instance, the development of a **common database of health images** by the Commission, in coordination with Member States. This image database purpose is to be dedicated to the most common forms of cancer, using AI to improve diagnosis and treatment. In addition, the **European High-Performance Computing Initiative (EuroHPC)** is pooling resources to develop the next generation of supercomputers to process big data and train AI. The Organisation for Economic Co-operation and Development (OECD, 2020) and the Council of Europe also published recommendations on AI considering the impact of algorithms-based systems on Human Rights (Zuiderveen Borgesius, 2020). The EIT Health Consultative Group (CG) provided views on policy issues specifically for health innovation that have been collected by the EU Commission or other EU institutions (Cohen et al., 2020; Gerke et al, 2020; EIT Health Consultative Group, 2020). Different existing EU regulations, standards and legislations match with the relevant principles described by the **European Commission's High-Level Expert Group on AI in their Ethics Guidelines of Trustworthy AI**.

3.2.2 Examples from Canada, US and UK

In the US, on October 12th 2016, the White House Office of Science and Technology Policy (OSTP) released the US report on AI, entitled "Preparing for the Future of Artificial Intelligence". The report presented the strategy of US regarding: (1) regulation of AI and when applicable the government should aim to fit AI into existing regulatory schemes; (2) importance of research and economic impact of AI on jobs; and (3) ethical issues related to AI (e.g., fairness, accountability, and social justice (Cath et al, 2018). Lately, the "National Artificial Intelligence Research and Development Strategic Plan" provided a detailed description and policy recommendations on "how to use R&D investments" towards the transformational impact of AI on the society (Gerke et al, 2020). More recently, in January 2020, the White House published draft guidance for the regulation of AI applications. The guide contains 10 principles that agencies should consider for AI-based systems development and implementation. These principles are: (1) public trust in AI; (2) public participation; (3) scientific integrity and

information quality; (4) risk assessment and management; (5) benefits and costs; (6) flexibility; (7) fairness and non-discrimination; (8) disclosure and transparency; (9) safety and security; and (10) interagency coordination (Gerke et al, 2020).

Regarding legislations for health-related information, the US has three federal legislations: (1) the **Privacy Act**; (2) the **Health Insurance Portability and Accountability Act (HIPAA)**; and (3) the **Genetic Information Non-discrimination Act (GINA)** (Ho et al, 2019; Stanfill et al, 2019; Carter et al, 2020).

1. The **Privacy Act** prevents “*unauthorised disclosure of personal information held by the US federal government, and the persons to whom the information relates*”.
2. **HIPAA** protects “*potential and current employees from discrimination by health insurers and employers*”, but it permits broad and easy dissemination of patients’ medical information, with no audit trails for most disclosures.
3. **GINA** expands the protection against certain discriminatory practices under HIPAA. It provides “*a level of protection against genetic discrimination by disallowing health insurers and employers to use certain types of genetic information*”, but it does not address the use of or access to genetic data.

The Food and Drug Administration (FDA) adopted a risk-based approach applied to the overall product lifecycle process. This approach is presented in the ISO 14971 standard, as well as in the guidance and technical report document ISO TR 24971. The standards outline the risk management process for medical device manufacturers, including the identification of hazards, the estimation and evaluation of risks and (Ho et al, 2019).

Moreover, the International Medical Device Regulators Forum (IMDRF) defines ‘Software as a Medical Device (SaMD)’ as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device.¹¹⁹ The FDA, under the Federal Food, Drug, and Cosmetic Act (FD&C Act) considers medical purpose as those purposes that are intended to treat, diagnose, cure, mitigate, or prevent disease or other conditions.¹²⁰ Thus when AI/ML is applied to the “treatment, diagnosis, cure, mitigation, or prevention of disease” the software is referred to as SaMD in the US¹²¹ (Angehrn et al, 2020).

The HIPPA address the issues of privacy and confidentiality by involving the cybersecurity aspect of the transference of information. Healthcare institutions must protect their systems and the personal data that is under their responsibilities. The HIPPA does not specify the measures to be implemented to comply with this requirement, but the FDA requires manufacturers and healthcare service providers to report the risks potentially present in their devices and take the necessary measures to ensure safety. These two regulations do not fully address the unique characteristics of AI-based systems such as unsupervised ML systems that learn and change (Ho et al, 2019).

Australia’s **Therapeutic Goods Regulation** is aligned with the EU regulations and legislations. The Therapeutic Goods Act 1989 (Cth) defines ‘therapeutic goods’ and ‘medical devices’ very broadly, particularly if therapeutic claims are made (Choy Flannigan, 2019).

¹¹⁹ Software as a Medical Device (SaMD): Key Definitions: <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>.

¹²⁰ See Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback <https://www.fda.gov/media/122535/download>

¹²¹ FDA (2019a). Clinical decision support software: Draft guidance for industry and Food and Drug Administration Staff, <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software> and Federal Food, Drug, and Cosmetic Act, Section 201(h). United States of America.

Box 26. Australia's Therapeutic Goods Regulation

Section 41BD of the Act defines 'medical device' as:

- (a) *any instrument, apparatus, appliance, material or other article (whether used alone or in combination, and including the software necessary for its proper application) intended, by the person under whose name it is or is to be supplied, to be used for human beings for the purpose of one or more of the following:*
- (i) *diagnosis, prevention, monitoring, treatment or alleviation of disease;*
 - (ii) *diagnosis, monitoring treatment, alleviation of or compensation for an injury or disability;*
 - (iii) *investigation, replacement or medication of the anatomy or of a physiological process control of conception;*
 - (iv) *and that does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but that may be assisted in its function by such means.*

Sources: Australia's Therapeutic Goods Regulation

During the legislative process of the **Data Protection Bill 2018 through the UK Parliament** there were attempts to strengthen the legal obligation to provide an explanation after a decision had been reached but these were unsuccessful (PHG Foundation, 2019).

The FDA intends to apply its regulatory oversight to mobile medical applications to those that only could pose a risk to the patient's safety in case the app does not work as intended. Therefore, the US FDA will not be able to regulate low risk devices if those do not gather, process, analyse or interpret medical data (PHG Foundation, 2019).

Box 27. Definitions of software as a device, by Section 3060 of the 21st Century Cures Act 2016

'Certain software is exempted from requirements for medical devices, including software that provides medical recommendations and the basis for those recommendations to health care professionals. Software remains subject to regulation as a medical device if: (1) the software acquires, processes, analyzes, or interprets medical information; or (2) the FDA identifies use of the software as reasonably likely to have serious adverse health consequences.'

Source: US FDA

To sum-up, Table 25 shows the different regulatory agencies and pathways for AI medical devices in USA, Europe and Canada.

Table 25. Regulatory framework for AI medical devices in the USA, Europe and Canada

Area	USA	Europe	Canada
Regulatory agency			
Organisation	FDA	Accredited private Notified Bodies; manufacturer's self-responsibility for low risk medical devices; mutual recognition between EU States, EFTA States, and Turkey	Medical Device Bureau (MDB) at Health Canada
Centralised or decentralised	Centralised	Decentralised	Centralised
Regulatory pathway			
Specific pathway for AI/ML-based medical devices	None	None; general requirements are safety, performance, and reliability; clinical studies generally assess high-risk devices; practice might vary across Notified Bodies, many instruments are foreseen to harmonise those practices. Proposed legislation on AIA and DGA.	None; current federal laws do not provide a level of protection suited to today's digital environment. Recently (January 2020) it has been launched a public consultation on to ensure the appropriate regulation of AI in the Personal Information Protection and Electronic Documents Act (PIPEDA). Legislative changes to PIPEDA are still required to help reap the benefits of AI while upholding individuals' fundamental right to privacy.
Premarket approval	Regulatory category for high-risk medical devices (class III); devices must provide valid scientific evidence from non-clinical and clinical studies showing safety and effectiveness	NA	NA
510(k) pathway	For class I, II and III medical devices for which premarket approval is not indicated; applicants must compare their device to one or more similar legally marketed devices; it can include non-clinical and clinical performance data	NA	NA
De-novo premarket review	For class I or class II medical devices for which general controls alone, or general and special controls, provide reasonable assurance of safety and effectiveness for the intended use	NA	

Source: adapted from Muehlematter et al. (2021)

In early 2019, the FDA released a proposed regulatory framework for AI/ML-based Software as Medical Device (SaMD) as a first step to regulate such devices. The aim being a potential approach to mandate premarket review for AI/ML-driven software modifications. The proposal discusses its experience in the premarket approval of "locked" algorithms. However, "adaptive" AI/ML-based SaMD with the ability to continuously learn and adapt to real-world data have not been able to be regulated using the traditional pathways. Suggestions were made as to whether a new total product lifecycle (TPLC) regulatory approach is required to keep up with the pace of

these highly iterative, autonomous devices while continually providing an effective and safe regulatory framework. The proposal anticipates that modifications to devices incorporating AI/ML may involve algorithm architecture modifications and re-training with new data sets. The types of modifications fall into three broad categories, namely clinical & analytical performance; inputs used by the algorithm and their clinical association to the SaMD output; and the intended use of the device for the state of the healthcare condition. The proposed regulation addresses the necessity of a TPLC approach by assessing the quality of a manufacturer's software development, testing, and performance monitoring of the device. This approach enables the continual evaluation and monitoring of a software product from its premarket development to post-market performance.¹²²

3.2.3 Current gaps

Approval, certification, and authorisation of AI systems in healthcare

Ensuring that AI health applications can meet the expectations of its use in healthcare, including the clinical outcomes, highlights the consideration of having a unification of good practices for integrating digital evidence approaches into authorization or certification common procedures between the main EU and international agencies (e.g., European Drug Agency, Food and Drugs Administration, Food Administration Agencies) (Diebolt et al, 2018; Stanfill et al, 2019).

The FDA is the agency that currently has the highest number of AI-based medical solutions and algorithms approvals. Its framework takes into consideration the risky nature of AI-based solutions and algorithms used in medical decision-making or medical data analysis within the approval and licensing process. The process of approval and licensing contemplate rigorous process that includes the compliant with a set of strict and specific regulatory requirements to receive approval and licensing within three levels of clearance: 510(k), pre-market approval, and novo pathway (Benjamens et al, 2020).

Box 28. FDA levels of clearance

510(k), is granted when it has been shown to be at least as safe and effective as another similar legally marketed algorithm.

Pre-market approval, is granted to algorithms for Class III medical devices, that can have large impact on human health and their safety and effectiveness evaluation undergo more thorough scientific and regulatory processes.

Novo pathway, is granted to novel medical devices without legally marketed counterparts, but that offer adequate safety and effectiveness with general controls.

Source FDA

Although the Food and Drugs Administration (FDA) does not establish official policies regarding AI use in the healthcare sector, they have developed a draft guidance attempting to create a framework that allows software to evolve and adapt to improve its performance (Lai et al, 2020; Esmaeilzadeh, 2020; Alami et al, 2020; Recht et al, 2020). Current regulatory frameworks are designed clear and approve locked algorithms that do not change their output over time when the same input is applied. In this regard , the FDA announced in 2018 that it is moving toward a pre-certified approach for AI adaptive algorithms that learns and improves continuously, ensuring that these changes still meet the gold standards for "*safety and effectiveness through the product's lifecycle*" provided by the FDA regulation, as well as developing a framework for classifying the risk associated with SaMD to finally regulate AI systems with a total product

¹²² It could be said that this FDA approach has influenced the AIA, where the notions of pre-defined algorithm changes and total lifecycle approach have been operationalised.

lifecycle regulatory approach (Yu et al, 2018; Fernandez et al, 2020; Paranjape et al, 2020; Benjamins et al, 2020).

According to Benjamins et al. (2020) the **FDA has cleared or approved around 64 AI-based medical devices and algorithms** (Benjamins et al, 2020). From these 64 developed for the fields of Radiology, Cardiology and Internal Medicine, 29 mentioned AI utilization in the official FDA announcement. From these 29, 25 were approved with a 510(k) clearance, 8 received the novo pathway clearance and only 1 received the pre-market approval (Benjamins et al, 2020). More recently, Muehlematter et al. (2021) searched governmental and non-governmental databases to identify **222 devices approved in the USA and 240 devices in Europe**. The number of approved AI/ML-based devices has increased substantially since 2015. Only a small fraction of the included AI/ML- based medical devices were qualified as high-risk devices. This could vary depending on how the proposed AIA will define high risk systems. However, the fact that there is a need to conduct specific searches in different databases to identify the number of devices cleared or approved reveals the level of maturity and transparency of the current landscape.

In April 2018, they authorized the first AI device to diagnose diabetic retinopathy without a physician's help in the USA. The FDA granted approval for IDx-DR (DEN180001) to be marketed as "*the first artificial intelligence (AI)-based diagnostic system that does not require clinician interpretation to detect greater than a mild level of diabetic retinopathy in adults diagnosed with diabetes*" (Ho et al, 2019). Other relevant examples include a medical imaging platform approved by the FDA (in 2017) as the first ML application to be used in clinical practice of cardiac magnetic resonance image analysis. This market authorization was granted by the FDA in 2018 to an image software called OsteoDetect that helps clinicians in detecting a common type of wrist fracture and HeartFlow® an advance diagnostic tool approved by FDA in 2019 (DEN130045) that generates a 3D model of a patient's heart and applies deep learning techniques to predict the impact of any blockages (Gerke et al, 2020; Angehrn et al, 2020).

Furthermore, since 2011 the **US Agency for Healthcare Research and Quality (AHRQ)** has compiled over 17000 algorithms and computer programs for healthcare evaluation, treatment, and administration purposes (Stanfill et al, 2019). There is a lack of evidence related to issues about certification, authorization, reimbursement of AI in healthcare within Europe. The **European regulatory regime adopts a risk-based approach** to regulate medical devices that are aiming to provide diagnosis, prevention, monitoring, treatment, or alleviation of diseases. The responsibility of risk assessment is placed on device manufacturers or on an independent certification body appointed by authorities of EU Member States (Ho et al, 2019). The new Medical Devices Regulation (MDR) requires CE certification through a notified body and requires a large increase in quality, safety and post-market surveillance (EIT Health Consultative Group, 2020). However, there are no targeted AI-specific requirements (Gilbert et al, 2020; Strohm et al, 2020, Fernandez et al, 2020). The proposed AIA fills this gap by introducing AI-targeted requirements for high-risk AI systems, which apply in conjunction with the medical device framework. The AIA operationalises the concept of product lifecycle approach and provides specific considerations for conformity assessment of self-learning AI systems. Certain aspects related to AI systems providing information are still unclear (see section 0).

In terms of certification, **EU and US methods are converging to determine whether a device is regulated as a medical device**. Both jurisdictions primarily look to determine whether a device qualifies as a medical or in vitro diagnostic device. (PHG Foundation, 2019). Furthermore, when referring to AI use in healthcare, the existing effort of the FDA regulation for treating software as a medical device (SaMD) can be considered as a reference point for the construction of an EU framework (Rowley et al, 2019; Baig et al, 2020). AI medical device

approval helps generate revenue for manufacturers, and clinicians can benefit from having more tools that would improve clinical workflow with potential impact on patient outcome (Pasapane et al, 2018). Currently, the paradigm is shifting from volume-based reimbursement to value-based reimbursement (Cinasi et al, 2019) where artificial intelligence tools must be adopted with the health goals of the population and the value-based payment structure as these systems are not reimbursed in the same way as traditional medicine services, following the current pay-for-service model (Golding et al, 2019). The three most common ways a medical procedure is reimbursed are: current procedure terminology codes and units of relative value, hospital outpatient prospective payment schedule, and business expenses. However, while AI is included, there is a need for the government to get reimbursement from private payers or providers as the mechanism is unclear (Schoppe, 2018). Nonetheless, economies continue to emerge that govern AI deployment, although there is still no clear answer on models and cost-effective reimbursement for these systems (Parkes et al, 2015).

Table 26 Rules on the conditions under which AI-based products are approved

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	Planned
Czechia	No	Netherlands	No
Denmark	No	Poland	No
Estonia	No	Portugal	No
Finland	No	Romania	No
France	No	Slovakia	No
Germany	No	Slovenia	No
Greece	No	Spain	No
Hungary	No	Sweden	Yes
Ireland	No		

Source: Author's elaboration

A vast majority of Member States did not report having any rules on conditions under which AI-based products are approved in place. Checking the figures provided by Muehlematter et al. (2021) (240 devices in Europe) or the analysis reported by Leuwne et al. (2020) (100 evaluated CE-marked products) it seems that manufacturers are using the MDR. However, most of the experts consulted stated that legal uncertainty is stopping manufacturers for bringing new AI-systems into the market.

At a Member States level, **only a few countries are currently implementing rules on AI-based product approval**. In Malta, the Maltese Digital Innovation Authority (MDIA) is developing a set of guidance notes aimed at assisting Service Providers and AI-ITA Applicants when approaching the MDIA for registration and certification respectively. In Czechia, while no draft regulations have been prepared, several relevant acts have been implemented, including the "Memorandum of cooperation on the development of AI", "Analysis of the Development

Potential of Artificial Intelligence”, “Innovation Strategy of the Czech Republic 2019–2030”, “National Artificial Intelligence Strategy (NAIS)”, “Regulatory Framework for Artificial Intelligence in the European Union”, and “Visegrad 4 countries”. In Sweden, the National Board of Health and Welfare's tools for structuring and coding information created the conditions for appropriate and structured documentation in health care and social services. The tools include the National Information Structure (NI), the concept system Snomed CT, health-related classifications and the National Board of Health and Welfare's term bank.

Under the EU Medical Device Regulations (MDR & IVDR) a manufacturer can only place medical devices, including AI-based devices, on the market for use on patients or their data when these are safe and effective. Once the device is on the market, the manufacturer must perform clinical evaluations throughout the entire lifetime of the device, including post-market clinical follow-up, to prove the assumptions remain valid and no risks emerge that are unacceptable. Devices that change during use can do so only within predefined boundaries considered during the conformity assessment procedure. For most of the medical software, a third party, a so-called ‘notified body’, performs the conformity assessment, both premarket (ex-ante) and post market (ex-post). The medical device regulations impose strict limitations with regards to the significance of changes allowed by the AI manufacturer before a new conformity assessment is required. The country factsheets inquired the existence of rules on evaluation of AI health applications.

Table 27. Rules on evaluation of AI health applications

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	No
Czechia	Yes ¹²³	Netherlands	No
Denmark	No	Poland	No
Estonia	No	Portugal	No
Finland	No	Romania	No
France	Yes ¹²⁴	Slovakia	No
Germany	No	Slovenia	No
Greece	No	Spain	No
Hungary	No	Sweden	No
Ireland	No		

Source: Author's elaboration

¹²³ Continuous evaluation of legislative and other legal risks for the competitiveness of the Czech Republic, creation of ethical frameworks and for the national implementation of binding EU regulations and recommendations.

¹²⁴ Development of an analysis grid of algorithms using artificial intelligence (AI) and in the MD that are subject to evaluation by the CNEDiMTS (National Authority for Health (HAS)).

Only two countries reported having rules on the evaluation of AI health applications in place: Czechia and France. The proposed AIA and DGA are intended to address the lack of regulation (see section 3.2.4)

Safety, technical robustness, and accountability

Regulatory frameworks concerning liability and safety of new products, as well as general safety and performance requirements, are defined by the **Product Liability, Machinery Directive**, the **Medical Device Regulation (MDR)**, **In Vitro Diagnostic Medical Devices Regulation** and **Article 22 of the General Data Protection Regulation (GDPR)** which replaced the Data Protection Directive of 1995, for access rights in case of 'automated decision-making' (Pesapane et al, 2018; Horgan et al, 2019; Schönberger, 2019; Alpalhão Gonçalves, 2018; Angehrn, 2019; Zuiderveen, 2020; ESR 2020; Gerke et al, 2020).

Box 29. GDPR Art. 22. Automated individual decision-making, including profiling

1. *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*
2. *Paragraph 1 shall not apply if the decision:*
 - (a) *is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
 - (b) *is authorised by Union or Member States law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
 - (c) *is based on the data subject's explicit consent.*
3. *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*
4. *Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

Source: GDPR

However, the application of AI in healthcare might not be fully solved as many of the challenges remain uncovered. The main risk regarding safety and technical robustness is the dependency of AI on large amounts of good quality, unbiased, standardised, and interoperable data. If the available data does not satisfy these minimum requirements, the potential of AI can be limited to be useful, accurate and safe and can lead to AI errors (EPF's Response & Accompanying statement, 2020). The proposed AIA, DGA and forthcoming EHDS will have to address these issues.

Box 30. AI systems training process

Experts interviewed in the area of AI research in the healthcare domain suggested that involving humans in AI training process, explaining the outcomes of the tasks, and sustain the responsible use of AI systems, may ensure the consumer that the AI assisted system is safe. However, there is a wide range of scenarios (see Figure 4) that might require some clarifications in order to reach adequate levels of safety. Healthcare professionals interviewed think that the level of reliability of an AI system need to be known. Experts are acknowledgeable that there is no system with 100% reliability (a 10-15% of uncertainty will always be there). However, health professionals need to know the level of error on which the decision should be taken, independently if the system is closed or progressive learning. Related to this, experts interviewed from industry consider that we are not really at the point to give a hight accuracy for the AI services in healthcare. In terms of guarantee and reliability, medical professionals consider that manufacturers should provide the warranty or reliability information that correspond to reality. For them, the most important is **to regulate that AI is an instrument with a level of guarantee and reliability that can vary greatly depending on how it is used, informing patients that the decision taken also consider information from an artificial intelligence system**. In addition, as regards to new implementations, medical experts consider that it must always be supervised by a team specialized the medical act. Considering that, when the level of effectiveness of the system has less possibility of error, it will be possible to gradually leave alone the automated system to make a decision, but after training and an overlapping phase of supervision with the automatic system. Aligned with the above, experts interviewed from industry believe in AI system if those are thoroughly tested, even though can be deployed without human supervision. To reach this AI autonomy, sufficient testing and the provision of enough evidence that AI is not going to harm lives is needed. The proposed AIA, EDG and the forthcoming EHDS might need to address all these issues (see section 3.2.4).

Sources: Authors' elaboration based on experts' opinion

Privacy, security and data governance

The right of self-determination and privacy, at a European level, is addressed by the Article 8 (1) of the European Convention on Human Rights (ECHR) and Article 7 of the European Charter of Fundamental Rights (Schönberger, 2019).

Box 31. European Convention on Human Right Art 7 and 8

European Convention on Human Right - Art 8(1): "*Everyone has the right to respect for his private and family life, his home and his correspondence*"

European Charter of Fundamental Rights - Art 7: "*Everyone has the right to respect for his or her private and family life, home and communications. Text: The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR.*"

Sources: European Convention on Human Right

The individual's **right of protection of their personal data** is set out by GDPR. Several articles of the GDPR can be applied when governing AI, and specifically AI use in the healthcare sector. AI developers and producers need to be transparent about the use of personal data by providing detailed information about all stages of algorithms decision-making processes involving personal data, to comply with GDPR principles. For ensuring that organisations comply with GDPR, a process called Data Protection Impact Assessment (DPIA) needs to be performed to assess systems when they could attempt against human rights and freedoms. This process systematically analyses, identify, and minimise the data protection risks. Regarding the data used for medical research or in medical practice, the application of GDPR is not always clear and

straightforward even though it considers this type of data as a special category of data and established safeguards for its protection. The GDPR provides requirements related to the explicit informed consent for handling health information, how is being processed, rectification of the data, and the right to "*a judicial remedy for any breach of these rights*" (Ho et al, 2019; Horgan et al, 2019; Zuiderveen Borgesius, 2020). Additionally, AI-based systems used in healthcare are not fully covered by the GDPR, because it does not consider some socio-technical challenges presented by machine learning and algorithms (Cath, 2018). Furthermore, Article 5 of GDPR brings principles of the processing of personal data (EIT Health Consultative Group, 2020).

Box 32. GDPR Art 5. Principles relating to processing of personal data8

1. Personal data shall be:
 - (a) *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')*
 - (b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')*
 - (c) *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')*
 - (d) *accurate and, where necessary, kept up to date...('accuracy')*
 - (e) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed... ('storage limitation')*
 - (f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures ('integrity and confidentiality')*
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Source: GDPR

Article 6 of GDPR provides the basis for data processing, and it is complemented by Article 9 covering the exceptions to the general rule prohibiting the processing of sensitive data set. Several Member States currently state that consent set out in Article 6(1)(a) and explicit consent set out by Article 9(2)(a) are the appropriate legal bases to be used for health-related research purposes. Nevertheless, others Member States prefer making public interest in public health or research, following Articles 9(2)(i) and (j). These different interpretations of the GDPR have led to fragmentation among Member States that has an impact on the implementation and research at the European level (EIT Health Consultative Group, 2020). Article 29 of GDPR complements it with the authority of the controller to enable data processing.

Box 33. GDPR Art 6 and 9

Article 6. Lawfulness of processing

Art 6(1): *Processing shall be lawful only if and to the extent that at least one of the following applies:* (a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*

Article 9. Processing of special categories of personal data

Art 9(2)(a): *the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member States law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;*

Art 9 (2)(i): *processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member States law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;*

Art 9 (2)(j): *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member States law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

Article 29. Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member States law.

Source: GDPR

The GDPR contains specific rules for certain types of "**automated individual decision-making**". Specifically, Article 22 (and Articles 13(1)(f), 14(1)(g) and 15(1)(h)), prohibits certain types of fully automated decisions with legal or similar significant effects. There are some exceptions of this rule, including cases where the individual "gave consent to the automated decision system, or if the decision is necessary for a contract between the individual and the data controller, or is authorised by law" (Vellido, 2019; Schönberger, 2019; Zuiderveen Borgesius, 2020).

Box 34. GDPR Art. 22, 13 and 14

Article 22. Automated individual decision-making, including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Article 13. Information to be provided where personal data are collected from the data subject

1. *Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:* (f) *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.*

Article 14. Information to be provided where personal data have not been obtained from the data subject

1. *Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:* (f) *where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers*

referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

Regarding **risk analysis** of systems, Article 35 provides regulations on aggravated risk analysis called "the data protection impact assessment". This assessment includes regulations to issues related to the type of processing, the cases when impact assessment is required, the necessity to provide a public list of the kind of processing performed, the compliance with the codes of conduct (Martinez, 2019).

Box 35. Article 35 - Data protection impact assessment

Art 35 (3): *A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*

- (a) *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
- (b) *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
- (c) *a systematic monitoring of a publicly accessible area on a large scale.*

The appropriate use and re-use of health data can improve health systems' sustainability, increase the quality, safety, and patient-centeredness of healthcare, improve access, decrease costs, and transform care into a more participatory process. Nevertheless, the pathway to reach these benefits is still not fragmented and not yet developed with patients' views. The regulation on European data governance (Data Governance Act - DGA) will serve as a horizontal framework for data governance across the different sectoral data spaces (see Lot 3). However, it will be desirable that the European Health Data Space (EHDS) framework will provide further legislation on the re-use of health data which will complement the general rules set out in the DGA. A solid governance framework, built on trust, data protection, ethical standards, transparency, and clear definitions will be fundamental to ensure the safe and efficient establishment of the health data space while increasing citizens' and patients' trust in data sharing. This requires also the harmonization and review of consent process (EPF's Response Statement, 2021).

Under the **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (CETS No. 108) people have the right to "*to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her*". Also, the GDPR contemplates the requirements of transparency of automated decision systems. Article 15 states that "*The controller shall provide the data subject with the following information (...) the existence of automated decision-making, including profiling (...) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*" Additionally, Article 5 of GDPR covers the lawfulness, transparency, and minimization of data, as well as guarantee the rights of access to data (Schönberger, 2019; Martinez, 2019).

Box 36. GDPR Art. 15 Right of access by the data subject

1. *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*
2. *Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.*
3. *The controller shall provide a copy of the personal data undergoing processing. 2For any further copies requested by the data subject; the controller may charge a reasonable fee based on administrative costs. 3Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*
4. *The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.*

Articles 13/14 of the GDPR require that a data subject is provided with meaningful information about the logic involved and the consequences of such processing. Article 12(7) suggests that standardized icons can be used to give an easily visible, intelligible, and meaningful overview of the intended processing. Limiting a counterfactual explanation to a specific case also means that it cannot demonstrate whether a system is operating fairly. If models are learning models, a counterfactual explanation will not inform future decisions (PHG Foundation, 2019).

Table 28. Rules on medical data gathering, organisation and use of medical data for developing AI in healthcare

	Yes/Planned*/No		Yes/Planned*/No
Austria	Yes	Italy	Yes
Belgium	Yes	Latvia	No
Bulgaria	No	Lithuania	Yes
Croatia	No	Luxembourg	Yes
Cyprus	No	Malta	No
Czechia	Yes	Netherlands	No
Denmark	Yes	Poland	No
Estonia	Yes	Portugal	Yes
Finland	Yes	Romania	No
France	Yes	Slovakia	Yes
Germany	No	Slovenia	Yes
Greece	No	Spain	Yes
Hungary	Yes	Sweden	No
Ireland	Yes		

Source: Author's elaboration

Results as to whether Member States implemented specific rules on medical data gathering, organisation and use of medical data for developing AI in healthcare are mixed. A majority (16) Member States have implemented such like rules, including Austria, Belgium, Czechia, Denmark, Estonia, Finland, France, Hungary, Ireland, Italy, Lithuania, Luxemburg, Portugal, Slovakia, Slovenia, and Spain.

Transparency and increased explainability on how AI algorithms work and, on which data sets are used to test, train, and validate algorithms, are fundamental to increase trust in artificial intelligence in healthcare (EPF's Response & Accompanying statement, 2020).

Experts from patients' associations (European Patient Forum) consider that trust is a barrier to AI digital solutions. The low trust in AI may be related to the limited knowledge on what and where actually AI applies in healthcare services. AI services are much linked to the interaction with the healthcare professionals for the patient, so the trust may be achieved with a clear explanation on the use of AI, not in terms of providing technical details to the patients but having the transparency level of at least knowing how it works. The level of the information available increase the level of trust. From a survey launched on AI to patients from the European Patients Forum, several respondents still do not know how AI could apply in health, so the knowledge on AI in health is still mainly basic. From this survey, patients mention as a key challenge the lack of transparency on how AI works (including quality of data), and they reclaim building knowledge in three levels: easily accessible 'basic' knowledge on how AI works in healthcare, knowing potential risks and your rights in case of errors, and knowing how AI outputs are used.

Similarly, healthcare professionals interviewed recognize essential to transmit to the health professionals the level of reliability of the tests and how they are done to allow interpreting results correctly in the context of the clinical environment with the rest of the variables. However, this implies that health professionals should have sufficient knowledge to understand this

information. Furthermore, there is still a lack of standards when addressing AI performance (see section 3.1.4). Having the appropriate training and standard procedures to assess and interpret the results will allow health professionals to derive the value from what artificial intelligence can contribute, as another instrument. Moreover, the more open the system, with the clearer criteria, incorporating AI in a transparent way in terms of mechanisms, the more security the professional will have. The use of AI information has to be based on transparency and it may be needed to regulate the process by which this information is generated. The information has to be suitable for who has to take the information. Standardization of language can be very helpful. Summarizing, transparency is a critical aspect for AI implementation in healthcare.

From industry perspective, the demand from any robust system is also to have full transparency between the AI systems and the health professionals. There should be a full transparency maintained in terms of the performance levels and the accuracies of these AI systems. Experts interviewed from industry highlights that the critical aspect is the patient trust and the ethical use of all the patient data must be tackled from very early stages. Furthermore, experts from law perspective, consider that the provision of information from the manufacturer to the injured party is part of the transparency obligation. When you have a regime that enforces that transparency, then the party can easily show what are the defects, so that should be embedded in the system through the transparency requirement. Below we report the results of the survey on the rules on access to algorithms used in healthcare as an example of the lack of regulation.

Table 29. Rules on the access to algorithms used in healthcare

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	No
Czechia	No	Netherlands	No
Denmark	No	Poland	No
Estonia	No	Portugal	No
Finland	No	Romania	No
France	No	Slovakia	No
Germany	No	Slovenia	No
Greece	No	Spain	No
Hungary	No	Sweden	No
Ireland	No		

Source: Author's elaboration

No country reported having rules on the access to algorithms used in healthcare in place that could serve to increase transparency of AI deployment. In addition, the survey inquired the existence of rules on the assessment of self-learning algorithms used in healthcare.

Table 30. Rules on the assessment of self-learning algorithms used in healthcare

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	No
Czechia	No	Netherlands	No
Denmark	No	Poland	No
Estonia	No	Portugal	No
Finland	No	Romania	No
France	Yes ¹²⁵	Slovakia	No
Germany	No	Slovenia	No
Greece	No	Spain	No
Hungary	No	Sweden	No
Ireland	No		

Source: Author's elaboration

As gets visible, no country reported having rules on the assessment of self-learning algorithms used in healthcare in place.

AI-based systems must be aligned with the ethics of human dignity focused on guaranteeing the fundamental rights. As explained in previous sections, algorithms functioning, and ways of training can lead to discrimination and other types of bias. This is specifically defined as digital discrimination or algorithmic discrimination (Hacker, 2018; Martinez, 2019; Schönberger, 2019; Zuiderveen Borgesius, 2020). The following regulations applies when seeking non-discrimination, diversity, and fairness of AI-based systems:

- **Art. 21 of the Charter of Fundamental Rights:** *Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.*
- Directive 2000/43/EC, the **Race Equality Directive**
- Directive 2000/78/EC, the **Framework Directive**, guards against discrimination based on religion or belief, disability, age, or sexual orientation in employment matters.
- Directive 2004/113/EC, the Goods and Services Directive: gender discrimination.
- Directive 2006/54/EC, the Gender Equality Directive.

¹²⁵ Development of an analysis grid of algorithms using artificial intelligence (AI) and in the MD that are subject to evaluation by the CNEDiMTS (National Authority for Health (HAS).

- **EU anti-discrimination law, Non-discrimination Law and Data Protection Law:** most relevant and main legal instruments for defending people against algorithmic decision-making discrimination
- **Article 14 of the European Convention on Human Rights** prohibits both direct and indirect discrimination. *"The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."*

Increasing reliance on AI and black box algorithms create potential challenges of opacity, bias, and discrimination. The GDPR is to enforce a harmonised data protection standard in the EU through regulation of the use of personal data and establishment of data processing principles (PHG Foundation, 2019). Biases in data also introduce ethical issues in terms of the potential for AI-enabled decisions themselves to be biased or discriminatory. Biases in data collection can affect the type of patterns AI will identify, for instance, specific population groups are often under-represented clinical trials and large data sets used to train AI. This needs to be reported to better understand the outcomes of the AI system. Appropriate requirements on data quality are contained in the AIA, including in relation to possible bias and discrimination. The forthcoming EHDS will also contribute to address these issues. Patients with multiple or rare diseases, and society in general, may also be affected by this. AI should also be used to develop solutions for health inequalities, including addressing social determinants of health, but also increasing equitable access to high-quality healthcare for all, in line with the fundamental shared values of European health systems (EPF's Response & Accompanying statement, 2020).

Experts from research on AI in healthcare interviewed concern about the bias included in an AI software when trained from one clinic and processed somewhere else, as the results could be different, and remark that AI solutions should be extended not only to regions but also to medical institutions, with different resolutions.

Liability and AI in healthcare

Several questions are still open regarding who should be held liable or accountable when healthcare-related decisions are made based on AI solutions. It is challenging to find a responsible actor since there are many actors involved in the creation and final use of an AI-based system for healthcare (e.g., developers, patients, healthcare professionals, manufacturers, etc.). It is important to define the responsibilities for the decisions AI algorithms produce. The following sub-sections discuss liability problems and current legal regulations to address responsibility issues between all actors (Stanfill et al., 2019; Rowley et al., 2019; Sullivan & Schweikart, 2019).

Determining who may be to blame for medical errors is typically straightforward: a misdiagnosis would likely be the fault of the overseeing physician; a patient harmed by a medical device would be able to sue the manufacturer or operator (Chung & Zink, 2017). Medical professions are regulated across the EU. Likewise, products and services in healthcare have a high implication and impact in patients' healthcare pathway and in standard of care and, thus, need to be strictly regulated by recognised authorities of the Member States. AI systems in health can be used across the health domain (see Figure 3) in several ways. Based on the AI system outcome and the level of expertise/qualification of the users, we have proposed four types of systems (see Figure 4), each type has also to consider the level of autonomy (fully automation, partial automation, AI assistance and shadow mode):

- Type 1. AI systems performing tasks or activities for individuals with knowledge expertise (qualified).
- Type 2. AI systems performing tasks for individuals with lay expertise (no-qualified).
- Type 3. AI systems providing information to individuals with knowledge expertise (qualified).
- Type 4. AI systems providing information to individuals with lay expertise (non-qualified).

A “medical device”, as defined by the EU, is a tool (including software) intended to be used for purposes that include diagnosis, prevention, monitoring, treatment, or alleviation of diseases (Ho et al, 2019). AI in healthcare could be considered as a medical device but some considerations should be addressed first, namely regarding the definition of “**software as a medical device (SaMD)**”. The International Medical Device Regulators Forum (IMDRF) defines SaMD as “*software intended to be used for one or more medical purposes that performs these purposes without being part of a hardware medical device*” (Ho et al, 2019; Gómez-González et al, 2020). But this definition does not foresee the intrinsic characteristic of some AI algorithms to be dynamically changing through self-learning, modifying their performance or functionalities (EIT Health Consultative Group, 2020) as is the case for continual learning system that feed from data accumulation and learn and improve from experience without being explicitly programmed (hence also referred to as black boxes). Furthermore, the **intended use** and therefore the AI system type, could play a key role too. These distinctions are relevant as potentially different models of liability apply to these systems yet again. On the question of whether traditional products liability frameworks continue to apply to the new generation of decision-making tools which enjoy high levels of autonomy and self-learning abilities, Chagal-Feferkorn (2019) notes that several regimes of liability rules have been offered, but these systems do seem to warrant their own custom-made treatment. The question is how these liability frameworks should look like to be able to respond effectively to these future advancements.

Article 2(1) of the Medical Devices Regulation defines medical device “*as any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:*

- *diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations”*

Thus, AI systems which **intended purpose** is under one of these categories could be considered as medical device. The proposed AIA regulation also mentions intended purpose as one of the key elements when regulating AI systems. Moreover, the MDR is also mentioned in relation to **safety components of products** (Recital 30) and to the classification of an **AI system as high-risk** (Recital 31). The EU provides regulatory frameworks concerning liability and safety of new products and technologies via the Product Liability and Machinery Directives (Horgan et al, 2019). Products recognised as medical devices commonly fall also within the scope of the

Product Liability Directive (Directive 85/374/EEC - adopted in July 1985). Product liability rules aim to maintain a fair balance between the interests of consumers and producers. The rationales behind products liability laws is that consumers can claim compensation for damage caused by defective products. If a defective product causes any physical damage to consumers or their property, the producer has to provide compensation irrespectively of whether there is negligence or fault on their part.¹²⁶ Importantly, the product liability directive does not refer explicitly to software, and thus its application depends on the question whether software can be regarded as a product.¹²⁷ To address this, the Commission published a report on the broader implications for, potential gaps in and orientations for, the liability and safety frameworks for artificial intelligence, the Internet of Things and robotics¹²⁸ and in 2021 an inception impact assessment and consultation process.¹²⁹

In broad terms, there are two ways software might constitute a product. Rather uncontroversially, if software is a component in a wider physical product, there will be a good claim against this composite product. Controversially, software that is not incorporated into a wider product (standalone software) might count as a product, but it is contentious whether software itself counts as a product for the purposes of product liability (Ordish, 2018). As suggested by Alheit (2001), the EU directive would apply in cases where damage is caused by a defect in the support material. In situations where software is transferred independently of material support by means of internet, cable, radio, etc. one may have argued that the EU directive would not apply, but if the software is incorporated into a material support, the EU directive would clearly apply. Such a distinction if it were to be applied it may lead to very unfair results for the victim to whom it really makes no difference in what form the software is acquired (Alheit, 2001). Additionally, some AI medical devices, and in concrete, those providing services (e.g., diagnostic advice to a physician), may not qualify as products for the purpose of the PLD and hence, do not fall under the products liability directive, which raises questions as to what liability regime applies instead.

According to the Medical Devices Regulations (EU) 2017/745 and 2017/746, "*software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device*" (Schonberger, 2019). The **MDR states that the intended purpose of the software is decisive for the categorisation of a software as a medical device** (Wiring, 2018). AI technologies with a medical purpose are required to ensure a high level of safety and performance demonstrating compliance with requirements on these regards defined by the MDR (Horgan et al, 2019).

In its ruling in the case SNITEM (Syndicat National de l'Industrie des Technologies Medicales) vs. Philips France, within which the qualification of software as medical device was discussed under Articles 1(1) and (2) of the Medical Devices Directive, the ECJ ruled that regardless of

¹²⁶ https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en

¹²⁷ Software has often been excluded from the ambit of product given its intangible nature, to which the product liability directive does not seem to apply (Alheit, 2001). As suggested by Alheit, the nature of the transaction causing the damage has to be distinguished from the rendering of a service, as a different European law regime applies to damage caused by defective services. In Anglo-American law the question whether software entails the rendering of a service or the sale of a product is solved by applying the 'essential nature test'.

¹²⁸ <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064>

¹²⁹ Civil liability – adapting liability rules to the digital age and artificial intelligence
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en

acting in the human body or not, the standalone software¹³⁰ in question¹³¹ was a medical device by stating that “software, of which at least one of the functions makes it possible to use patient-specific data for the purposes, *inter alia*, of detecting contraindications, drug interactions and excessive doses, is, in respect of that function, a medical device (...) even if such software does not act directly in or on the human body”. In light of this judgement as well as of the content of both the new Medical Devices Regulation and guidelines on the application of the 'MEDical DEVices' Directives (MEDDEVS 21/6), there is little margin to still affirm that AI medical decision support software does not qualify as a medical device. However, **the reservations upon the applicability of the defective product's liability regime still remain for AI-based medical devices providing information** (Reutiman, 2012). A particular gap in this respect concerns AI systems that provide information (services), such as medical diagnosis but also well-being information to clinicians and/or individuals.

Importantly, liability for medical errors falls under tort law. A tort is a civil claim in which a party requests damages for injuries caused by a harmful, wrongful act of another (Sullivan & Schweikart, 2019). Patients may recover compensatory and punitive damages from physicians, health care organizations, pharmaceutical companies, and medical device manufacturers if they are injured as a result of the failure to meet judicially accepted standards. Typical tort claims in the realm of medicine and health include medical malpractice (negligence), *respondeat superior* (vicarious liability), and products liability. In the case of damage or harm caused due to a defect or error coming from medical device, the Directive 85/374/EEC Product Liability Directive (PLD), and its national local implementations, might apply in parallel to a negligence action. Under this directive, “...a producer is liable for damage caused by a defect in his product”, knowing as a defect “any deviation from the standard of safety which a person is entitled to expect” and “do not offer the safety that a person is entitled to expect, considering all circumstances”, including the presentation of the product, its reasonably expected use and the time in which it was put into circulation (Art. 6 PLD) (European Commission, 2019; European Parliament, 2020). Manufacturers can mitigate risk by insuring against tort liabilities, which works well when the individualized liability risks of different manufacturers collectively balance out in the pool of policyholders.

As indicate above, there continues to exist legal uncertainty as to **whether some types of AI systems qualify as products for the purposes of the PLD**. Academics have raised concerns as to whether algorithms that replace human discretion can and should be classified as “products, regardless of products liability rationales, and damages caused by such algorithms may be attributed to defects” (Chagal-Feferkorn, 2019). It could be the case that Type I and II AI systems, **AI systems performing tasks** (see Figure 4), are closer to a product while Type III and IV, **AI systems providing information to individuals** could be considered services

The legal uncertainty over whether algorithm-based software satisfies the definition of a product is not unique (Ordish, 2018). Three algorithm-based software characteristics might exacerbate this legal uncertainty:

- First, given the **potential opacity of future machine learning software**, proving fault in a regular negligence claim may be difficult, especially when it comes to AI system

¹³⁰ Under MEDDEV “stand alone software’ means software which is not incorporated in a medical device at the time of its placing on the market or its making available.”

¹³¹ The Philips’ software under assessment had the purpose of “cross-references patient-specific data with the drugs that the doctor is contemplating prescribing, and is thus able to provide the doctor, in an automated manner, with an analysis intended to detect, in particular, possible contraindications, drug interactions and excessive dosages, is used for the purpose of prevention, monitoring, treatment or alleviation of a disease.”

providing information. Health professionals are used to take decisions and explain why these decisions were taken. However, in AI software providing services (e.g., decision support system to a radiologist) it could be the case that the AI system produces an outcome (e.g. a recommendation) with limited reasoning attached. Furthermore, in many cases it could be difficult to disentangle the AI model from the date used to feed the model (see section 3.1.3).

- Second, under the current PLD, if machine learning software that is incorporated into a product makes the product defective and cause damage, it is possible to get compensation from the producer of the product. However, since software is not currently qualified as a product in its own right, it is not possible to get compensation from the producer of the software.¹³² Therefore, whether an AI system is part of a medical device or whether it is a medical device in its own right might play a role in how liability is approached;¹³³
- Third, if a machine learning algorithm leads to a **faulty or delayed diagnosis or treatment**, the liability for any resulting injury may be extremely costly. Furthermore, this could be also related to the data used no to the algorithm itself.

Nowadays, there is a considerable debate at European level regarding the applicability of the PLD to AI-based tools and non-embedded software. Furthermore, as regard of AI-based products, the legal framework presented in the PLD does not suit and cover all the necessary issues caused by a new generation of systems (e.g., robots) equipped with adaptive and learning abilities (Schönberger, 2019; European Commission, 2019). According to Chagal-Feferkorn (2019), self-learning algorithms are inherently expected to cause damage regardless of any defects. This is because sophisticated systems, in particular self-learning algorithms, rely on probability-based predictions, and probabilities by nature inevitably get it wrong some of the time. This raises important questions, including how this type of AI will be implemented in healthcare settings (e.g., warnings, alerts, decision support systems...) considering the end user expertise/qualification (qualified expertise vs. lay expertise) and the level of control (from fully automation to shadow mode). Medicine as application domain is considered among the greatest challenges of artificial intelligence and machine learning. In medical decision support, we are confronted with uncertainty, with probabilistic, unknown, incomplete, imbalanced, heterogeneous, noisy, dirty, erroneous, inaccurate and missing data sets in arbitrarily high-dimensional spaces (Holzinger, Dehmer, & Jurisica, 2014). Explainability of AI could help to enhance trust of medical professionals in future AI systems. Research towards building explainable-AI systems for application in medicine requires to maintain a high level of learning performance for a range of ML and human-computer interaction techniques. There is an inherent tension between ML performance (predictive accuracy) and explainability. Often the best-performing methods such as DL are the least transparent, and the ones providing a clear explanation (e.g., decision trees) are less accurate (Bologna & Hayashi, 2017). This raised the importance of how AI is developed and implemented (see section 3.1.3) and how its performance is assessed (see section 3.1.4) together with the role of data governance (see section 3.2.4).

A relevant study commissioned by the European Parliament is the study¹³⁴ on a civil liability regime for artificial intelligence – European added value assessment, which presents the main

¹³² Study on Safety and Liability Related Aspects of Software (see <https://digital-strategy.ec.europa.eu/en/library/study-safety-and-liability-related-aspects-software>)

¹³³ For example, the Apple Watch has only been evaluated for the detection of AFib or normal sinus rhythm and is not intended to detect any other type of arrhythmia. It cannot detect heart attacks (see https://www.accessdata.fda.gov/cdrh_docs/reviews/DEN180044.pdf)

¹³⁴ [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654178/EPRS_STU\(2020\)654178_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654178/EPRS_STU(2020)654178_EN.pdf)

points of discussion relating specifically to the application of **Product Liability Directive (PLD)** to the new technologies as summarised below:

Table 31. The main points of discussion relating to the application of PLD to AI

PLD Concept	Issue	Open questions/problems
Product	Scope of the definition	Should PLD cover all tangible and non-tangible items (including software)? The current formulation is not clear and divergent opinions exist as to the definition of software (is it a product or a service?)
Defect	Notion of the defect as central element of liability determination	The current formulation of a defect in the PLD is closely related to the concept of safety. It is not clear what would be the safety expectations, for example, in relation to cybersecurity and AI. The concepts of defect and safety, as well as notions of reasonable and expected use, might need thorough revision if software is to be included explicitly within the scope of the PLD
Damage and burden of proof	Type of damages covered	The type of damages covered is not harmonised. The scope of pure economic loss and non-material damage are highly contested. It might be excessively difficult and prohibitively costly for a consumer to prove a defect exists, especially, for complex technological applications. Therefore, the burden of proof concept might need to be addressed to ensure balanced distribution of a burden between the parties.
Producer	Scope of liable persons	Who should be a liable person for the purposes of the PLD? What should be the role of the different economic operators in the value chain? Specific producer? Software designer? To what extent should a producer be liable, for example, for third party software or applications installed in the product? Should joint liability of all actors involved be applied?
Exemptions and defences	Time limitation and exemptions that limit liability of the producer	10-year rules for the expiry of claims might be problematic. Moreover 'the development risk defence' might need to be clarified.

Source: EP (2020) based on the EC Expert Group

The **Report on liability for Artificial Intelligence and other emerging technologies prepared by the Expert Group on Liability and New Technologies** in November 2019 covered strict liability of producers for defective products regulated by the Member States themselves. On a national level, it can generally be observed that the laws of the Member States do not (yet) contain liability rules specifically applicable to damage resulting from the use of emerging digital technologies such as AI.

The harmful effects of the operation of emerging digital technologies can be compensated under existing ('traditional') laws on damages in contract and in tort in each Member States. Furthermore, given the significant differences between the tort laws of all Member States, the outcome of cases will often be different depending on which jurisdiction applies. As experience with the Product Liability Directive has shown, efforts to overcome such differences by harmonising only certain aspects of liability law may not always lead to the desired degree of uniformity of outcomes.

Table 32 reports the results for liability rules that were adopted for AI products and services in healthcare in each Member States. As gets visible, a vast majority did not implement any specific liability rules that were adopted for AI products and services in healthcare. Malta is currently working on a Private Law Bill aiming to clarify IP and liability issues. Portugal is currently considering the creation of an ethical committee for AI and Automation to define and deploy guidelines for ethical-by-design AI. Slovak law does not distinguish between physicians' liability in case of provision of health care using telemedicine and liability in case of provision standard health care. The Action Plan on the Digital Transformation for 2019-2022 intends to establish a Permanent Commission on the Ethics and Regulation of AI, which should deal with the issues related to liability for damage.

Table 32. Liability rules that were adopted for AI products and services in healthcare

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	Planned
Czechia	No	Netherlands	No
Denmark	No	Poland	No
Estonia	No	Portugal	Planned
Finland	No	Romania	No
France	No	Slovakia	Yes
Germany	No	Slovenia	No
Greece	No	Spain	No
Hungary	No	Sweden	No
Ireland	No		

Source: Author's elaboration

3.2.3.1.1 Safety insurance (CE mark)

A key question in the development of software solutions is the regulatory classification of the product. It is especially vital to clarify whether the software is a medical device. This is important from a practical point of view because medical devices can only be marketed if they carry a CE label, which they receive after having undergone a conformity assessment procedure. If a product that qualifies as a medical device does not have CE labelling, a competitor could demand that the product be withdrawn from the market. Moreover, it would represent an administrative offence and may even have consequences under criminal law.

The MDR and IVD regulations emphasise a life-cycle approach to safety, backed up by clinical data. For MDs, all Class IIa, IIb and III as well as some specific Class I require the intervention of a Notified Body (MDR Article 52(7)(a4, b5, c6). MDR Article 52 and MDR Annexes IX, X and XI describe the different assessment routes according to the class of the device. In some cases, manufacturers can choose their conformity assessment route from several options described in the Regulation. The assessment of the conformity of a device for CE marking (Conformité Européenne, or European Conformity) varies according to the risk class for both MDs and IVDs.

Apart from the risk classification, certain features may influence the conformity assessment procedure, for example when an MD is required to be sterile, or an IVD is designed for use by patients. There is uncertainty about how the proposed AIA risk based approach will intersect with the MDR. The classification under the medical device framework will be decisive in making an AI system high-risk under the AIA, given that the AIA considers high-risk any AI system regulated by relevant sectorial legislation which is subject to third-party conformity assessment. The proposed AI system typology sketched in Figure 4 incorporates several examples to exemplify how the AI systems in healthcare could be placed depending on the AI system outcome and the level of expertise of the user. The intended purpose will play a key role when considering both the AI system type and the specific class (Annex VIII, Chapter II Implementing rules, 3.1. Application of the classification rules shall be governed by the intended purpose of the devices). The AI in healthcare it is still on its infancy from a regulatory perspective (van Leeuwen et al., 2021).

3.2.3.1.2 Challenges to current liability frameworks

Ideally, AI should offer health care professionals and patients options and better results, and the science should be in the service of humans and of the good of society (Aluas, Maniac & Vaida, 2019). However, there may be instances of adverse effects arising from the use of AI systems that bring up important questions related to liability. **Advances in the use of AI in healthcare such as machine learning may challenge the existing legal position whereby clinicians are liable for AI-aided software malfunctions that contribute to inaccurate or delayed diagnosis.** In many jurisdictions, the case law has developed in relation to software used to support rather than make clinical decisions, which allows patients to claim actions for clinical negligence. Given the potential opacity of future machine learning software, proving fault in a regular negligence claim may be difficult, especially in the cases of AI systems providing information. However, there exist legal uncertainty over whether machine learning software satisfies the condition of a product. For instance, following the classification described in Figure 4 (see section 3.1.2), AI systems performing tasks for individuals (Type I and II) are closer to a product than AI systems providing information (Type III and IV) that could be considered as services. This could be the starting point to clarify the differences between AI systems in health with respect to liability, considering the asymmetries of information between the different actors (see section 3.1.2). The intended purpose again will play a key role.

When **AI-enabled software systems take over aspects of healthcare involving a level of 'intelligent' assessment, it is important that the risks and corresponding potential liabilities are fully understood and managed appropriately.** Transparency is important also for regulators who may require clinical AI tools to be explainable to clinicians to whose decision making they are coupled; to quality assurance officers and IT staff in a health provider organization who acquire the clinical AI and have risk-management/legal responsibility for their operation; to developers; to regulators; or to other humans.

As outlined above, it is less than clear in many countries how product liability law applies to services rather than products. While a patient who suffers harm as a result of a defective monitoring device may well be able to recover under existing product liability regimes, he or she might have more difficulty recovering where information provided by e.g. an online advisory service was inaccurate. In light of significant challenges in applying the current tort framework to AI, legal and computer science experts have offered possible solutions that involve modifications to the current law or the creation of new legal doctrines let us take a look at these solutions and your opinion on these suggestions. In the EU, for example, the product liability

directive has been found to apply only to products and not to services¹³⁵. If damage is attributable to a service, it is therefore possible that the claimant will be unable to rely on a no-fault action and will instead be forced to pursue a claim under negligence. In many cases, AI systems would be medical devices and hence subject to the medical devices regulations. In addition, AI systems in healthcare would be also subject to obligations that would be set at EU level via the proposed AIA, the DGA and the forthcoming EHDS (see section 3.2.4).

3.2.3.1.3 Liability issues in case of harm to patients

Liability for medical errors falls under tort law. A tort is a civil claim in which a party requests damages for injuries caused by a harmful, wrongful act of another. Patients may recover compensatory and punitive damages from physicians, health care organizations, pharmaceutical companies, and medical device manufacturers if they are injured as a result of the party's failure to meet judicially accepted standards. Typical tort claims in the realm of medicine and health include medical malpractice (negligence), respondeat superior (vicarious liability), and products liability. **The law of tort of EU Member States is largely non-harmonised, with the exception of product liability law under Directive 85/374/EC**, some aspects of liability for infringing data protection law (Article 82 of the General Data Protection Regulation, GDPR), and liability for infringing competition law (Directive 2014/104/EU). Under the baseline scenario (i.e. no action taken), the current liability frameworks at EU and at national levels could be inhibiting the development and deployment of these technologies as **there are a number of uncertainties in determining liability for AI in health**. Consequently, manufacturers of AI, physicians using AI and patients subjected to AI medical systems might be unwilling to embrace AI. Below we articulate some of these uncertainties in more depth.

The proposed **AIA will apply extraterritorially to any provider or distributor of AI whose services or products reach the EU market**. This includes providers and users of AI systems outside the EU if the output of the AI system is used in the EU, including those deployed in medical devices. The AIA mandates an ex-ante conformity assessment for high-risk AI applications. In other words, AI systems—regardless of being products or services—in high-risk sectors need to be compliant with the AIA's obligations before they are placed on the EU market. The AIA considers two fundamental categories of high-risk: (1) AI systems related to regulated products. In particular an AI system is high-risk if it is a safety component of a product, if it is covered by one of 19 specified pieces of EU NLF single market harmonization legislation (e.g. machinery, medical devices), and the product is subject to third-party assessment under that legislation; and (2) Specific high-risk uses of AI systems as listed in Annex III in the AIA act. **To develop or use a high-risk AI system, an organization must meet a range of technical and regulatory requirements before the system can be brought to market**. This includes establishing safeguards against various types of biases in data sets, using prescribed data governance and management practices, ensuring the ability to verify and trace back outputs throughout the system's life cycle, incorporating provisions for acceptable levels of transparency and understandability for users of the systems, and appropriate human oversight over the system generally. There are further ongoing compliance obligations once the system is in the market

Currently, the Product Liability Directive 85/374/EEC (PLD) establishes a harmonized system for compensating consumers that suffered damage/injury from defective products. **However, many questions remain open especially in cases where AI systems provide health and care information/opinions (services)**, as they are not currently covered by the PLD.

¹³⁵ See Cases C-65 para- 36 <https://curia.europa.eu/juris/liste.jsf?lgrec=fr&tde=%3BALL&language=en&num=C-65/20&jur=C>

The basis of proving “defect”, is laid down in Article 6 of the products liability directive and refers to “the safety which a person is entitled to expect”; another basis referred to in the US is the so called “risk-utility” test. The question arises as to what test a defect should be defined, and how it can be best structured to fit AI. Another question that needs to be considered is the type of liability that should be applicable for “faulty” medical information, such a diagnosis, generated by digital means (including those based on AI) that leads to adverse effects. In answering these questions, it must be considered that the mistakes that an AI medical system makes might be significantly different from the ones made by a human physician. Consequently, it can be argued that the overall performance of the algorithm needs to be considered in determining defect instead of the individual decision in every particular case.

Another important question is what type of warnings/instructions a manufacturer should provide to the physician who is using AI systems. It could be necessary to include some form of explanations on why the AI system provides the particular prediction. The question arises as to when at a technical level the AI system contains a warning defects (warning defect means that no adequate warning was given of the inherent risks of the product; no warning was given as to how the product will function; consumer did not have the information on how the product will function in order to allow the consumer to decide whether or not to use the product), but also what type of warnings would it be suitable for AI in health. Lastly, an important question touching **liability issues is the decision as to when an ML system in health can be said to malfunction, that is, in which situations we could argue that an AI system in medicine “departs from its intended design” and purpose.** For example, when the AI system has been hacked or contains a software bug, it has to be clarified whether the manufacturer should be held strictly liable as presume that that product is defective and hence manufacturer liable. Nevertheless, for AI systems that provide medical information (advice) e.g. to a physician, the allegation could be that the faulty information provided by the AI system was not the cause of the patient’s injury/ death. The manufacturer could be claiming that it was the clinician who caused the death/injury of the patient. This creates **uncertainties as concerns liability in cases of injuries/death when AI has been used in for example treatments.**

Two different options could be implemented to clarify the issue of causation. A first option would be to use a test of “foreseeability” that should be incorporated at EU level in determining causation in these circumstances. In other words, if it was foreseeable that the physician/patient would have relied on the information generated by the AI system then the chain of causation should not be broken. A second option would be to expressly mention at EU level that causation should not be broken when AI systems provide specialised information to physician/patient. In all cases, it is important to consider the asymmetry of information in the health domain and therefore the level of expertise of user (qualified vs no-qualified expertise).

An important question in the event of an injury/ death caused by the use of the AI systems in healthcare provision is further whether the plaintiff bears the burden of proof to show that the AI system has been defective and that it was the cause of the adverse effects. Under the PLD, the plaintiff bears the burden of proof. However, this burden might be heavy, as it is not always easy to trace back the injuries caused by AI systems. An important question to address is therefore how injured parties can be supported to prove their case in the event of harm. A last question concerns cases in which a physician used an AI system according to the instructions and warnings provided by the manufacturer and the physician is not negligent in any other way, the physician should still be still liable for AI adverse effects. In order to answer these questions, there is a need to establish a data governance structure and transparent phases to monitor not just the use of the AI system into the market but also the whole development process (see Figure 5 in section 3.1.3).

3.2.3.1.4 Continuous learning AI

AI in medicine is classically not continuously learning (ie. does not adapt by itself after its deployment in real settings). In the cases where AI continues learning and adapting after its deployment in real healthcare settings, it has to be clarified whether any regulatory obligations on the manufacturer and doctor be set when it is deployed in healthcare provision. Machine learning as a form of continuous learning AI is a technology that allows computers to learn directly from examples and experience in the form of data. Some concerns have been raised that machine learning could foster the growth of black box medicine, where clinical decision making becomes increasingly opaque. Techniques such as machine learning do not easily lend themselves to human concepts of explanation and significance, while its outputs are typically probabilistic and sometimes inscrutable. Given the opaque nature of black-box AI, key questions emerge when confronted with possible medical malpractice caused by such technology.

Under the AIA, mandatory post-market monitoring obligations for high-risk systems are imposed. Serious incidents or faults of the AI system which breach safety laws or fundamental rights must be reported to the national supervisory body. In case of a violation of the Act, regulators can mandate access to the source code of a high-risk AI system. High-risk systems that violate the Act can be forcibly withdrawn from the market by the regulator.

3.2.4 The new EU proposals

During 2020, the EC has launched several initiatives that could provide the grounds to address some of the challenges (see section 3.1.5) and gaps (see section 3.2.3) previously mentioned. It is worth mentioning that health data play a critical role in the wide scope, characteristics and type of AI systems' use in health (see section 3.1.2) and the way these are developed, implemented (see section 3.1.3) and assessed (see section 3.1.4).

In February 2020 the EC announced the **European strategy for data**¹³⁶. This communication outlines a strategy for policy measures and investments to enable the data economy for the coming five years so "*the EU can become a leading role model for a society empowered by data to make better decisions – in business and the public sector*". The vision includes the aim "*to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value*". In order to make this vision a reality, the Communication recognizes the need to "*combine fit-for-purpose legislation and governance to ensure availability of data, with investments in standards, tools and infrastructures as well as competences for handling data*", ensuring that:

- *data can flow within the EU and across sectors;*
- *European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected;*
- *the rules for access to and use of data are fair, practical and clear, and there are clear and trustworthy data governance mechanisms in place; there is an open, but assertive approach to international data flows, based on European values.*

Better healthcare and healthier lives are mentioned in the Communication as one of the areas that could clearly benefit from this strategy. Moreover, **health is one of the strategic areas where sectoral data spaces are considered**.

¹³⁶ COM/2020/66 final https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf

The importance of health data has been also emphasised in the **Proposal for a Regulation on European data governance (Data Governance Act)**¹³⁷. This proposal would address the following situations:

- *Making public sector data available for re-use, in situations where such data is subject to rights of others.*
- *Sharing of data among businesses, against remuneration in any form.*
- *Allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).*
- *Allowing data use on altruistic grounds.*

Furthermore, it mentions that "sector-specific legislation can develop, adapt and propose new and complementary elements, depending on the specificities of the sector, such as the envisaged legislation on the **European health data space**".

Box 37. Data Governance Act. Subject matter and scope (Art. 1)

(1) This Regulation lays down:

- (a) conditions for the re-use, within the Union, of certain categories of data held by public sector bodies;
- (b) a notification and supervisory framework for the provision of data sharing services;
- (c) framework for voluntary registration of entities which collect and process data made available for altruistic purposes.

Source: Data Governance Act

As it is stated in the Inception Impact Assessment launched by the EC,¹³⁸ the **European Health Data Space (EHDS)** is "a Commission priority that aims at making the most of the potential of digital health to provide high-quality healthcare and reduce inequalities. It should promote access to health data for research and innovation on new preventive strategies, as well as on diagnosis and treatment of diseases to improve health outcomes, while ensuring that citizens have control over their own personal data." More concretely, EHDS regulatory framework will aim at:

1. **Ensuring access, sharing and optimal use of health data** for healthcare delivery purposes as well as re-use for research and innovation, policy-making and regulatory activities, in a privacy-preserving, secure, timely, transparent and trustworthy way, and with an appropriate institutional governance;
2. **Fostering a genuine single market in digital health**, covering health services and products, including tele-health, tele-monitoring and mobile health;
3. **Enhancing the development, deployment and application of trustworthy digital health products and services**, including those incorporating artificial intelligence in the area of health.

To fulfill these objectives, the new framework should cover some of the areas related to **AI systems development and implementation** (see section 3.1.3 and Figure 5). By ensuring access, sharing and optimal use of data the new regulatory framework should clarify how (2.i) access, analysis and assessment of the raw data; (2.ii) data collection process; (2.iii) data

¹³⁷ COM(2020) 767 final

¹³⁸ See [https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares\(2020\)7907993](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares(2020)7907993)

preparation and (2.iv) data transformation could be deployed "*in a privacy-preserving, secure, timely, transparent and trustworthy way, and with an appropriate institutional governance*". This should include guidelines about the selection and preparation of the data sets **to perform the selected models** (Phase 3), including training, validation and test and therefore the **evaluation methods** (the verification and validation of the models using the Test data set should be conducted – Phase 4) and potentially the requirements to deploy **AI systems in real settings** (Phase 5). This will also benefit clarifying the information needed to develop the technical requirements and will help developers to better describe the objectives and purpose of the AI system (Phase 1).

Ensuring access, sharing and optimal use of health data within the same EU regulatory framework will facilitate fostering single market in digital health as researchers and innovators will be applying the same approach and therefore decreasing potential barriers at Member States level. A common EU regulatory framework should also detail, considering other relevant regulations, the relevant **monitoring and surveillance measures** (5.ii) to be implemented by the **Competent bodies (Art.7)**. The inception impact assessment before mentioned envisages the analysis of "*the designation of national digital health bodies, which would be the sectoral counterparts of authorities supervising data intermediary services and working on interoperability (...). Moreover, in the same framework, sectoral bodies dealing with secondary use of health data, including data altruism, could be set up at national level and could be brought together at EU level*".

It is worth emphasizing that to achieve the current aims of the EHDS regulatory framework such a scheme should go beyond voluntary bases (see chapter 5 for more information). Furthermore, the development and implementation of AI systems in health and the exploitation of its potential could be limited by how the **conditions for re-use (Art. 5)** are defined and rolled out at Member States level. For example, pre-processed data (Art.5(3)) might not be sufficient to achieve specific evaluation metrics' level (see Table 21). Imposing obligations related to access and re-use of data within a secure processing environment (Art.5(4)) might limit specific types of techniques (see section 3.1.1) and therefore the evaluation metrics or even the objective of the AI system. These conditions make critical the type of support that the competent bodies will offer (Art.7(2)) and might create inequalities and disadvantages among competent bodies. These could be further exacerbated or levelled the importance of the role of the **Providers of data sharing services (Art.9)** and **Data altruism organizations (Art.15)** in health.

After the publication of the Data Governance Act, on 21 April 2021 the European Commission published its draft regulation on artificial intelligence ("**Artificial Intelligence Act**"¹³⁹) providing a horizontal regulatory framework that encompasses any AI systems developed and used within the single market. In light of the speed of technological change and possible challenges, the AIA confirms that the EU is committed to strive for a balanced approach to regulate future uses of AI systems horizontally. The horizontal nature of the proposal requires full consistency with existing Union legislation applicable to sectors where high-risk AI systems are already used or likely to be used in the near future. The proposed Artificial Intelligence Act (AIA) is notable for a comprehensive definition of AI which is line with a definition of AI developed by the OECD, and key requirements including extensive documentation, data quality, record keeping, human oversight, accuracy, robustness and cybersecurity.

¹³⁹ COM(2021) 206 final

Box 38. AIA Subject matter (Art. 1)

This Regulation lays down:

- (a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;
- (b) prohibitions of certain artificial intelligence practices;
- (c) specific requirements for high-risk AI systems and obligations for operators of such systems;
- (d) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;
- (e) rules on market monitoring and surveillance.

Source: Artificial Intelligence Act

The AIA defines AI broadly as a suite of software development frameworks that encompass machine learning, expert and logic systems, and Bayesian or statistical approaches. A software product featuring these approaches whose outputs "*influence the environments they interact with*" will be covered¹⁴⁰. **Following a risk-based approach, the AIA distinguishes three categories of AI uses: prohibited AI uses, high-risk AI uses, and systems with limited risk.**

The list of **prohibited practices comprises all those AI systems whose use is considered unacceptable as contravening Union values**, for instance by violating fundamental rights. The Act explicitly bans AI systems that use subliminal techniques to **manipulate a person's behaviour in a manner that may cause psychological or physical harm**.

The regulation also mentions that other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the existing data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice not to be subject to profiling or other practices that might affect their behaviour. The proposal also prohibits AI-based social scoring for general purposes done by public authorities. Finally, the use of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply¹⁴¹.

In order to develop or deploy a high-risk AI system, a provider's organization must meet a range of technical and regulatory requirements before the system can be brought to market. This includes establishing safeguards against various types of biases in data sets, using prescribed data governance and management practices, ensuring the ability to verify and trace back outputs throughout the system's life cycle, incorporating provisions for acceptable levels of transparency and understandability for users of the systems, and appropriate human oversight over the system generally (Centre for Data Innovation, 2021).

Thus, the whole AI system development pipeline (see Figure 5) including data governance will be shaped by the AIA. For high-risk AI systems which are components of a product (or products by themselves) covered by existing sectorial harmonization legislations (e.g. medical devices), **the requirements of the AIA will be checked as part of the existing conformity assessment procedures under those sectorial legislations**. This will have an impact on the

¹⁴⁰ Ibid.

¹⁴¹ COM(2021) 206 final

MDR and the way **software as a medical device** (SaMD) and AI system will be designed, developed and marketed. The EDHS is aimed to support the application of the AIA rules. The operational of AIA rules will rely significantly on standardisation and regulators' guidance.

The proposed AIA mentions high level of protection of health as one of the main overriding reasons of public interest in its first recital. It also mentions the potential of the AI systems to produce beneficial outcomes in healthcare as example (Recital 4). Thus, the AIA legal framework "*laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law*" (Recital 5).

Recital 28 emphasises that "*AI systems could produce adverse outcomes to health and safety of persons, in particular when such systems operate as components of products.*". It is not clear whether this also applies in the case as "components" of a service (see section 3.1.2): for instances when a doctor or other health professional will take a decision based on the outcome of an AI system. However, it is clear that in both cases, the risk-based approach is confirmed by the fact that the same recital states that "*in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate. The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk*". Thus, the level of autonomy and the individuals involved in the use of AI system might play a key role in defining the level of risk of the system in the health domain (see Figure 4. AI systems typology in section 3.1.2).

This remarks the importance of the definition of the **intended purpose** (see Recital 32) of the AI system that might determine whether an AI system in health is considered or not high risk. For example, an AI triage system used in an emergency department of a hospital shall be considered as high risk not just because its inherent risk but also because it might determine whether or not the individual will receive public assistance or establish priority in the dispatching of emergency (see Recital 37).

Recitals 43, 44, 45 and 46 address issues related with data and the **process to develop AI systems**. They clearly show the importance of a detailed approach to AI in health, starting by how AI systems could be defined in the field (see section Box 24. AI systems in health proposed definition), the potential typology (see Figure 4. AI systems typology) and how these systems could be designed, developed, assessed, deployed and monitored in real settings (Figure 5. AI system phases in health).

Due to the characteristics of health products and services (e.g. asymmetries of information, the level of autonomy, level of expertise) the interpretation of the system output and use (recital 47), the overview of the functioning by a natural person (recital 48), the appropriate level of accuracy, robustness and cybersecurity (recital 49), the resilient against risks connected to the limitation of the system (recital 50) and the specific responsibilities (recital 58) might need to be customised in a way that fits the peculiarities of the health sector. This could be further elaborated within the future EHDS considering other current EU legislations (see section 3.2.1) and the current gaps (see section 3.2.3).

For example, Art. 3 enumerates several definitions that might need to be further embedded within the context of health. The EHDS could provide more details on which concrete elements are needed in the case that AI systems in health are (11) 'putting into service', including (15) 'instructions for use', ways of (16) 'recall of an AI system' and the level of (17) 'performance of an AI system'. The last item might have implications for the reimbursement model too.

Moreover, the EHDS envisages the creation of data authorities that might play a role in defining (19) 'notifying authority', (21) 'conformity assessment body', (22) 'notified body' as well as (27) 'harmonised standard', (28) 'common specifications', (29) 'training data', (30) 'validation data', (31) 'testing data' and (32) 'validation data' due to its characteristics (see sections 3.1.2 and 3.1.3).

4. Governing the use of health data

4.1 Scoping the field

4.1.1 Analysing the value of health data

Health data scope. Across the Member States there is a rich and diverse collection of health data and medical data, which are held in electronic form (European Medicines Agency, 2019). These electronic data can include Electronic Health Records (EHRs), laboratory information with diagnostic data, medical images, prescribing data, dispensing data, data from disease registries, vaccination data, health determinant data, datasets from (non-)interventional studies and of civil registrations including cause of death. Literature on health data specifically highlights the relevance of multiple types of *data* (Marjanovic et al. 2017; EC 2014a; EC 2014b), including: (i) *EHR*, which can contain information on symptoms, medical exams, tests, referral patterns, prescriptions and death records as well as pharmacy records, diagnostic procedures, hospitalisations and other healthcare services; (ii) *claims data* giving indications of the nature of service usage, insurance and other administrative hospital data; (iii) *omics data*: genomics, transcriptomics, proteomics, epigenomics, metagenomics, metabolomics, nutriomics; (iv) *clinical trials data*; (v) *pharmaceutical data* such as pharmacovigilance (medicines safety) data; (vi) *social media including web data* pertaining to health such as data from patients forums on health topics; (vii) *mobile apps, telemedicine and sensor data*; (viii) *geospatial health data* (health data disaggregated by location); (ix) *ambient data* from 'smart' environments (e.g. electricity and gates data on the way people walk which can be used to estimate the occurrence of falling); (x) *information on well-being, socio-economic, behavioural data*; and (xi) *other records* of relevance to health such as occupational records, sociodemographic profiles or environmental monitoring data such as on pollution.

Quantifying the value of data is quite complex as it is dependent on many variables. Table 33 shows the characteristics that act as inputs to analysing the impact of the value of a data set. The characteristics shown in the table act as components for when estimating the value of EHRs, as shown in the next two subsections.

Table 33. Framework for analysing characteristics that impact the value of a data set

Objectives	Services
Nature	<ul style="list-style-type: none"> • Data type (patient, payer, product, provider, and scientific research) • Data availability or time frame (contemporaneous vs. historical with time lag) • Exclusivity or scarcity (available from a single source vs. multiple) • Granularity or detail (aggregated vs. transaction level) • Source or seller (original source/generator of the data vs. reseller)
Data quality, maturity and embedded analytic insight	<ul style="list-style-type: none"> • Raw (unorganised with potential data gaps and inconsistencies) • Curated (i.e. organised and easy to work with) • Aggregated longitudinally for the same patient or record • Analysed with descriptive statistics, insights and predictions or forecasts provided
Complexity of data capture	<ul style="list-style-type: none"> • Source of the party generating the data • Accessibility of data (open source vs. paid) • Data capture (auto-captured vs. collected with human intervention)
Use/application	<ul style="list-style-type: none"> • Use and potential impact • Exclusivity (exclusive license vs. data being offered to multiple buyers) • Limitations on use • Usage by other businesses or competitors

Source: EY (2019)

Health data sharing comprises many stakeholders, the most relevant in the context of this study being patients, medical professionals, policymakers, researchers, the pharmaceutical industry, the health IT industry, health technology assessment (HTA) bodies, notified bodies, and regulators such as European Medicine Agency (EMA) and national medicines agencies. The role that these stakeholders play is dependent on their access to and use of the health data, in particular whether it is direct access to health data for primary care (primary use) or re-use of initially collected health data for further purposes such as research, policy making or regulatory decision-making (secondary use).

In the health data space, patients or consumers (such as users of health apps) act as data contributors as well as users of this data. Third party users of the health data include researchers, policy makers, businesses and regulators. Prior to outlining the objectives and areas of this study, it is crucial to define the use of health data for primary and secondary purposes, respectively.

Use of health data for primary purposes. The use of health data for primary purpose in this report is defined as the data processing for the purposes of provision of health and social care by health and care providers to the patient concerned. This concerns data that is collected directly from a patient in the context of health and social care provision for the purpose of providing health or care services to that patient. This includes both in-person care and telecare using eHealth or mHealth tools (EC, 2020). Primary purposes include, but are not limited to, the following:

- Management of the health care of individual patients by healthcare providers and patients
- Monitoring the health care of individual patients by healthcare providers and patients
- Engagement in their own health care by individual patients
- Manage and administer hospital and health care service delivery
- Keep track of healthcare costs including billing for goods and services delivered
- Ensure reliable and consistently high quality of care.¹⁴²

Use of health data for secondary purposes. The use of health data for secondary purposes is defined, in the "Assessment of the Member States' rules on health data in the light of GDPR" (EC, 2020), as health data collected for an initial purpose being re-used for either of the following functions:

- Data processing for wider public health purposes including planning, management, administration and improvement of health and care systems; prevention or control of communicable diseases; protection against serious threats to health and ensuring high standards of quality and safety of healthcare and of medical products and medical devices.
- Data processing for scientific or historical research by both public and private sector organisations (third parties, not being the original data controller), including the pharmaceutical and medical technology industries and insurance providers.

¹⁴² Srinivasan, U. (2017, July 05). Primary and Secondary Uses of Health Data. Retrieved October, 2020, from <https://flyingblind.cmcrc.com/researchers/primary-and-secondary-uses-health-data>

When considering secondary usage of health data, examples of uses can include the following¹⁴³:

- Inform health system policy
- Research of drug utilisation studies such as use in different age groups (children) and off-label use;
- Safety monitoring and evaluation of drugs and treatments;
- Safety monitoring and evaluation of cross-border health threats;
- Planning and conduct of observational safety and effectiveness studies;
- Extrapolation of adult data to children or elderly;
- Identification of unmet medical needs;
- Assessing disease incidence/prevalence;
- Establishing differences in clinical practice;
- Measuring background rates of events (for assessment of drug safety);

Considering the areas mentioned below, the objectives of the study will be divided by whether they are addressed in the context of the use of health data for primary purposes or whether they fall within the context of health data re-use for secondary purposes.

Estimated total market value and market value per patient of EHRs. Taking into consideration Table 33, characteristics that impact the value of health data, we have conducted an exercise to estimate the total market value and market value per patient of EHRs. It is important to note that this is only a method to quantify the potential benefits of health data by estimating the economic value that could be generated. This is solely a method to estimate figures based off of a market price. In fact, the OECD Report “Exploring the Economics of Personal Data”¹⁴⁴ has divided methods assigning a monetary value to personal data into two classes: based off of market valuation or based off of individuals’ valuation¹⁴⁵. When considering market valuation, possible measures are (Czechik, 2017):

- Market capitalization, revenues or net income per data record (i. e., a company’s market capitalization, revenues or income divided by number of personal data records used by the company)
- Market prices for data (i. e., price for data record in data broker market)
- Cost of a data breach (i. e., cost incurred by a company or individual to recover from a data breach)
- Data prices in illegal markets

In this section, we base the value of health data on the above measures. Furthermore, all estimations are detailed in Annex 8.5.1. The estimates for total market value and per patient value of primary health records were based off of values in the 2019 EY report “Realising the value of healthcare data: a framework for the future” which estimated the value of primary care health records in the UK, specifically the health data held by the UK’s National Health Service.

¹⁴³ European Medicines Agency. (2020). The General Data Protection Regulation : Secondary Use of Data for Medicines and Public Health Purposes, A Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures (Vol. EMA/194011/2020, Rep.).

¹⁴⁴ OECD, “Exploring the Economics of Personal Data,” in OECD Digital Economy Papers, 2013.

¹⁴⁵ This does not, by all means, indicate that the European Commission endorses the selling of data.

The framework of estimating the value of patient data comes from Table 33. Additionally, this report used the following methods to quantify the value of data:

1. A market-based approach, calculating the implied “per record” valuation multiples of comparable data assets or valuation multiples of companies with significant patient assets.
2. An income-based approach, which quantifies value based on the economic benefit to be generated from the curated data set.

The total market value framework, calculated by EY, also considers that the benefits can impact a number of stakeholders, such as patients, physicians, pharmaceutical companies, medical device manufacturers and researchers. From this report, the value of these EHRs was estimated to be between €24–€217 per EHR (EY, 2019) in 2018¹⁴⁶. The total number of longitudinal primary health records or EHRs in the UK was estimated to total 55 million and therefore the total curated NHS data set was valued at several billion pounds with a realisation of £9.6bn per annum in benefits (i.e., the NHS benefits worth €5.7bn per annum and the patient benefits worth €5.2bn per annum). These are considered potential savings for the UK’s NHS generated by potentially enhanced patient outcomes, creation of wider economic benefits to the UK, development and use of ‘big data’, artificial intelligence and personalised medicine.

Box 39. Significance of estimating total market value of health data

Analysing the total market value of health data can support the prioritisation of health care by Member States, specifically when considering quality of care, cost-efficiencies, and preventative care. This market value comes from potential realized benefits such as medical breakthroughs for treating diseases, greater access and improvement to personalized medicine; greater efficiency in healthcare planning and delivery and/or evidence of cost-effectiveness and outcomes to inform value-based payments.

Source: Author’s elaboration

Based on the EY 2019 report, we considered the UK value per EHR as a baseline, with €24 based as the low range and €217 as the high range. See Annex 8.5.1 for a detailed description of how these values were calculated. First the number of primary health records available for Member State were extrapolated by considering their eHealth adoption index (EC, 2018) and population. The eHealth adoption index, which was valued in the “2018 Benchmarking Deployment of eHealth among General Practitioners” of the European Commission, represents the availability and adoption of eHealth across Member States. For context, this composite index takes into consideration four components: electronic health record adoption, health information exchange adoption, telehealth adoption, and personal health record adoption¹⁴⁷. The estimated value of each sub-component is shown in Annex 8.5.2. From there, the low and high range value of EHRs per patient were computed for each country’s purchasing power parity (PPP), which takes into consideration the differences in living costs between Member States. To find the total market value ranges, the number of patient records were multiplied by the relevant value for each patient record. These estimations are shown Table 36, with the final estimates resulting in low and high ranges for the market value in PPP national currency units/Euro per patient as well as the total market value.

¹⁴⁶ Values have been converted to EUR based off of the 2018 average conversion rate of 1£ =1.13EUR.

¹⁴⁷ The sub-indices have been calculated in the the Annex. Please note that each of the four sub-index contributes 25% to the total composite index (eHealth adoption index).

When looking at the results, Denmark, Finland, and Sweden have the highest potential economic value of EHR per patient, with high range values estimated at 340, 278, and 264 PPP national currency units / euro, respectively. The differences in the value of EHRs per patient differs by Member State due to their eHealth adoption index, population, and differences in living costs. This value could translate into the potential benefits such as benefits in research and medical breakthroughs, greater efficiency in healthcare planning, and improvement in personalised medicine, among many others.

With respect to the total estimated market value of EU health data, when considering the average eHealth adoption index across the EU, the value is estimated as between 6 and 55 billion PPP national currency unit / euro. When looking at the high range of the total market value of Member States, Germany has a potential total value of 13.4 billion followed by France with 8.9 billion, and Italy with 8.2 billion PPP national currency units/ euro. As stated in Box 39, this estimated market value derives from the potential benefits gained from the improvement of personalised medicine, greater healthcare planning efficiency, and medical breakthrough among others. However, it is important to note that fully realising these potential benefits also means overcoming challenges presented with digital health products and services such as securing data privacy and confidentiality. These risks need to be mitigated and addressed through quality control training, legal framework, and standardisation across all EHR users.

As for the total benefits per patient per annum and the estimated total savings per Member State per annum, this is shown Table 37. The total estimated savings for health services in the EU are valued at 4.6 billion PPP currency unit/ euro. The estimated economic savings for patients in the EU, when considering the average eHealth adoption index across the EU, is estimated to have a value of 4.3 billion PPP national currency /euro. As will be mentioned in the next few paragraphs, this translates to benefits on the quality-adjusted life years of patients from a reduction in disease and economic burden.

The baseline of this extrapolation follows the other tables, it uses the UK as a baseline; EY found that the NHS benefits would be worth €5.7bn per annum and the patient benefits would be worth €5.2bn per annum. The benefits, or economic savings, were estimated in the EY report by a methodology that combined expert consultation and literature review. This methodology split the economic uplift into three categories of impact – ‘big data’, AI, and personalised medicine (PM), with the short, medium, and long-term impacts found in Table 34.

Table 34. Realisation of the economic benefits resulting from the creation of an NHS longitudinal patient-level data set

	Big data	AI	Personalised Medicine
Short term (less than 3 years)	NHS bodies procure technology they need	Data set created and leads to useful insights on best practice	Pharma begins process of developing new medicines
Medium term (3-9 years)	Best practices and learnings spread through NHS	Best practices in short run implemented across NHS	New medicines go through clinical trials
Long – term (greater than 10 years)	All potential benefits realised	Continued discovery of useful insights	New medicines come to market

Source: EY (2019)

In detail, the following three categories and their benefits were considered:

- ‘Big data’ takes into consideration the benefits of having a longitudinal, single, and analysable patient-level data set.

- AI includes the benefits of applying AI to the longitudinal, single, patient-level data set such as improving patient outcomes through improved monitoring and better use of medicines, improve diagnostics, reduce errors, and as a secondary impact, positively impact public finances.
- Personalised medicine, through the 'big data' set mentioned previously, would benefit patients through the increased efficiency of medicines and technology and would benefit the NHS by reducing the number of inefficient treatments for patients, and therefore dedicating less resources to inefficient procedures or treatments. Personalised medicine benefits, according to the EY report, also includes revenue gains by life science companies that introduce new medicines and a better cost-efficiency by pharmaceutical companies, which could reduce the length and cost of clinical trials by targeting the correct patients for clinical trials.

As shown in Table 35, the reported economic values of these categories were estimated in the EY report.

Table 35. Summary of economic value to the UK NHS benefit to patients

Big data	AI	Personalised Medicine
NHS - €3.1bn per annum (p.a.)	NHS – €1.9bn p.a. Patients - €2.8bn p.a.	NHS – €0.7bn p.a. Patients – €2.4bn p.a.
Total NHS savings = €5.7 bn p.a. and total patient savings = €5.2bn p.a.		
Short-term benefits realisation from year 1	Medium-term benefits realisation from year 3	Long-term benefits realisation from year 10

*Values were converted from British pounds to euros based off of the average 2018 currency rate.

Source: EY (2019)

With regards to benefits per patients per annum, it is important to emphasize that benefits include **long-term impacts to quality-adjust life years** such as the reduction of disease burden for patients and economic burden for patients (more productive, increased consumption). As a summary, these are considered potential savings generated by potentially enhanced patient outcomes, creation of wider economic benefits, development and use of 'big data', artificial intelligence and personalised medicine.

Table 36. Estimated market value of health data per country

Country	Population (2018)**	eHealth adoption (2018)***	# of primary health records	€ value low range per patient	€ value high range per patient	% health records/ population	PPP National currency units/ Euro****	Market value in PPP National currency units/Euro per patient		Total market value in PPP National currency units/Euro (millions)	
								Low range	High range	Low range	High range
Austria	8,901,064	1.914	5,554,219	18	165	62%	1.09	20	181	110	1,003
Belgium	11,522,440	2.067	7,764,689	19	178	67%	1.11	22	198	168	1,540
Bulgaria	6,951,482	1.809	4,099,729	17	156	59%	0.50	9	78	35	321
Croatia	4,058,165	2.180	2,884,200	21	188	71%	0.69	14	129	41	371
Cyprus	888,005	1.934	559,901	18	167	63%	0.88	16	146	9	82
Czechia	10,693,939	2.063	7,192,437	19	178	67%	0.72	14	128	100	919
Denmark	5,822,763	2.862	5,432,977	27	247	93%	1.38	37	340	202	1,848
Estonia	1,328,976	2.785	1,206,650	26	240	91%	0.81	21	195	26	235
Finland	5,525,292	2.644	4,762,728	25	228	86%	1.22	30	278	145	1,324
France	67,320,216	2.054	45,080,122	19	177	67%	1.11	21	196	966	8,828
Germany	83,166,711	1.941	52,627,677	18	167	63%	1.03	19	173	993	9,080
Greece	10,718,565	1.785	6,237,550	17	154	58%	0.84	14	130	88	808
Hungary	9,769,526	2.028	6,459,228	19	175	66%	0.64	12	112	79	723
Ireland	4,964,440	2.103	3,403,680	20	181	69%	1.30	26	236	88	804
Italy	59,641,488	2.185	42,485,335	21	188	71%	1.00	21	189	878	8,026
Latvia	1,907,675	1.826	1,135,649	17	157	60%	0.74	13	117	15	133
Lithuania	2,794,090	1.647	1,500,283	16	142	54%	0.66	10	93	15	140
Luxembourg	626,108	1.776	362,519	17	153	58%	1.26	21	193	8	70
Malta	514,564	1.695	284,347	16	146	55%	0.84	13	122	4	35
Netherlands*	17,407,585	2.714	15,402,368	26	234	88%	1.11	28	260	437	3,999
Poland	37,958,138	1.837	22,732,814	17	158	60%	0.58	10	92	228	2,082
Portugal	10,295,909	2.118	7,109,348	20	183	69%	0.86	17	156	122	1,111
Romania	19,328,838	1.788	11,267,107	17	154	58%	0.54	9	83	103	940

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

Country	Population (2018)**	eHealth adoption (2018)***	# of primary health records	€ value low range per patient	€ value high range per patient	% health records/ population	PPP National currency units/ Euro****	Market value in PPP National currency units/Euro per patient		Total market value in PPP National currency units/Euro (millions)	
								Low range	High range	Low range	High range
Slovakia	5,457,873	1.756	3,124,547	17	151	57%	0.82	14	124	42	387
Slovenia	2,095,861	1.998	1,365,203	19	172	65%	0.85	16	146	22	199
Spain	47,332,614	2.365	36,494,782	22	204	77%	0.94	21	191	763	6,978
Sweden	10,327,589	2.522	8,491,476	24	217	82%	1.22	29	264	245	2,244
EU-27	447,058,422	2.089	307,333,495	20	180	69%	1.00	20	180	6,059	55,395
United Kingdom (baseline)	67,025,542	2.517	55,000,000	24	217	82%	1.16	28	252	1,513	13,836

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement between Estonia and Finland.

** Source: The World Bank website <https://data.worldbank.org/>

*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.

**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the aforementioned source and divided by the EU 2018 average of 102.9.

Source: Authors' elaboration

Table 37. Estimated total savings for Member States health services and benefits per patient per annum

Country	Population (2018)**	eHealth adoption (2018)***	# of primary health records	€ health saving for government services per annum (millions)	€ benefits for patients per annum (millions)	% health records/ population	PPP National currency units/ Euro****	Total savings for MS health services per annum in PPP National currency units/Euro (millions)	Total benefits for patients per annum in PPP National currency units /Euro (millions)
Austria	8,901,064	1.914	5,554,219	4,296	3,953	62%	1.09	4,701	4,325
Belgium	11,522,440	2.067	7,764,689	4,640	4,269	67%	1.11	5,163	4,750
Bulgaria	6,951,482	1.809	4,099,729	4,061	3,736	59%	0.50	2,040	1,877
Croatia	4,058,165	2.180	2,884,200	4,894	4,502	71%	0.69	3,353	3,084
Cyprus	888,005	1.934	559,901	4,341	3,994	63%	0.88	3,814	3,509
Czechia	10,693,939	2.063	7,192,437	4,631	4,260	67%	0.72	3,326	3,060
Denmark	5,822,763	2.862	5,432,977	6,424	5,910	93%	1.38	8,859	8,151
Estonia	1,328,976	2.785	1,206,650	6,252	5,751	91%	0.81	5,067	4,662
Finland	5,525,292	2.644	4,762,728	5,935	5,460	86%	1.22	7,239	6,660
France	67,320,216	2.054	45,080,122	4,611	4,242	67%	1.11	5,099	4,691
Germany	83,166,711	1.941	52,627,677	4,357	4,008	63%	1.03	4,493	4,133
Greece	10,718,565	1.785	6,237,550	4,007	3,686	58%	0.84	3,372	3,102
Hungary	9,769,526	2.028	6,459,228	4,552	4,188	66%	0.64	2,915	2,682
Ireland	4,964,440	2.103	3,403,680	4,721	4,343	69%	1.30	6,152	5,660
Italy	59,641,488	2.185	42,485,335	4,905	4,512	71%	1.00	4,919	4,526
Latvia	1,907,675	1.826	1,135,649	4,099	3,771	60%	0.74	3,051	2,807
Lithuania	2,794,090	1.647	1,500,283	3,697	3,401	54%	0.66	2,422	2,228
Luxembourg	626,108	1.776	362,519	3,987	3,668	58%	1.26	5,037	4,634
Malta	514,564	1.695	284,347	3,805	3,500	55%	0.84	3,187	2,932
Netherlands*	17,407,585	2.714	15,402,368	6,092	5,605	88%	1.11	6,761	6,220
Poland	37,958,138	1.837	22,732,814	4,124	3,794	60%	0.58	2,384	2,194
Portugal	10,295,909	2.118	7,109,348	4,754	4,374	69%	0.86	4,071	3,745
Romania	19,328,838	1.788	11,267,107	4,014	3,693	58%	0.54	2,173	1,999

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

Country	Population (2018)**	eHealth adoption (2018)***	# of primary health records	€ health saving for government services per annum (millions)	€ benefits for patients per annum (millions)	% health records/ population	PPP National currency units/Euro****	Total savings for MS health services per annum in PPP National currency units/Euro (millions)	Total benefits for patients per annum in PPP National currency units /Euro (millions)
Slovakia	5,457,873	1.756	3,124,547	3,942	3,626	57%	0.82	3,225	2,967
Slovenia	2,095,861	1.998	1,365,203	4,485	4,126	65%	0.85	3,796	3,493
Spain	47,332,614	2.365	36,494,782	5,309	4,884	77%	0.94	4,979	4,580
Sweden	10,327,589	2.522	8,491,476	5,661	5,208	82%	1.22	6,883	6,332
EU-27	447,058,422	2.089	307,333,495	4,693	4,318	69%	1.00	4,693	4,318
United Kingdom (baseline)	67,025,542	2.517	55,000,000	5,650	5,198	82%	1.16	6,550	6,026

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement between Estonia and Finland.

** Source: The World Bank website <https://data.worldbank.org/>

*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.

**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the beforementioned source and divided by the EU 2018 average of 102.9.

Source: Authors' elaboration

Estimated costs of data permit authority. The fixed costs for setting up a data permit authority were extrapolated in this report using FIndata as a baseline. It is important to note that, as for previous estimations, all table calculations are detailed in Annex 8.5.1. In 2019, the Finnish Government allocated 2.5 million euros for the year to launch the operations of the data permit authority and the construction of a data-secure environment. The budget is about 1 million euros per year, though it is higher in the beginning years 2019-2021 (EC, 2020). As shown in Table 38, the estimated costs of implementing a data permit authority within a year in other countries followed a similar exercise as the previous section; the estimations were calculated using the eHealth indicator and PPP. To compare the figures, it is important to give context of the funding for other data permit authorities. For comparison, the French Health Data Hub (HDH) was granted initial funding of 36 million euros for four years (EC, 2020). The values estimated are different due to many factors including the differences in staff between FIndata and the HDH; FIndata had 15 staff currently working for FIndata in 2020 whereas the HDH had about 50 staff members. In addition to the fixed cost, FIndata also provides public information about pricing that could be considered as a proxy for the variable cost of running the services:

- Fee for FIndata data request or data permit;
- Costs incurred by data controllers for the extraction and delivery of data, based on each controller's own regulations;
- Working hours used by FIndata for combining, pre-processing, pseudonymising and anonymising the data; and
- Remote access environment charge for data permit holders.

In the estimation for this report, these FIndata prices (with examples shown Box 40) are considered as variable costs and were the baseline for the estimation of costs for other Member States. The prices were divided into low and high ranges and from there were converted into PPP national currency units/Euro. The result of this estimation is shown in Table 39.

Box 40 Examples of fees for FIndata data permits and requests

The following permits and requests are included in the list of fees for FIndata

- Da data permit and data request related to a thesis for an applicant who is domiciled in Finland or another EU or EEA country: EUR 250.00
- Data permit for an applicant whose place of business is not in an EU or EEA country: EUR 3,000
- Processing costs for an expiring data request or data permit application (the amount of work already done is charged for data requests which are cancelled after processing has begun or for which the required additional information is not submitted): EUR 75/hour
- FIndata processing fee (hourly fee for data combining, pre-processing, pseudoanonymisation, and anonymisation): EUR 115/hour
- Remote access environment package S (small): 8 GB RAM, 4 Cores: EUR 187.50 / month
- Remote access environment package XL: 64 GB RAM, 8 Cores: EUR 460.42 / month

Source: FIndata (2021)

Table 38. Estimated fixed cost of data permit authorities

Country	Population (2018)**	eHealth adoption (2018)***	# of primary health records	Estimated fixed cost of data permit authority (thousands) Euro	% health records/ population	PPP National currency units****	PPP National currency units/ Euro	Estimated cost of health data permit authority PPP National currency units/ Euro (thousands)
Austria	8,840,521	1.914	5,563,354	1810	63%	112.60	1.09	1980
Belgium	11,427,054	2.067	7,765,897	1954	68%	114.50	1.11	2175
Bulgaria	6,951,482	1.809	4,134,594	1710	59%	51.70	0.50	859
Croatia	4,087,843	2.180	2,930,000	2061	72%	70.50	0.69	1412
Cyprus	1,189,265	1.934	756,227	1829	64%	90.40	0.88	1607
Czechia	10,629,928	2.063	7,210,186	1951	68%	73.90	0.72	1401
Denmark	5,793,636	2.862	5,451,772	2706	94%	141.90	1.38	3732
Estonia	1,321,977	2.785	1,210,503	2633	92%	83.40	0.81	2134
Finland (baseline)	5,515,525	2.644	4,794,741	2500	87%	125.50	1.22	3049
France	67,320,216	2.054	45,463,496	1942	68%	113.80	1.11	2148
Germany	82,905,782	1.941	52,908,719	1835	64%	106.10	1.03	1892
Greece	10,732,882	1.785	6,298,998	1688	59%	86.60	0.84	1420
Hungary	9,775,564	2.028	6,518,185	1918	67%	65.90	0.64	1228
Ireland	4,867,316	2.103	3,365,470	1988	69%	134.10	1.30	2591
Italy	60,421,760	2.185	43,407,193	2066	72%	103.20	1.00	2072
Latvia	1,927,174	1.826	1,157,014	1727	60%	76.60	0.74	1285
Lithuania	2,801,543	1.647	1,517,078	1557	54%	67.40	0.66	1020
Luxembourg	607,950	1.776	354,999	1679	58%	130.00	1.26	2122
Malta	484,630	1.695	270,083	1603	56%	86.20	0.84	1343
Netherlands*	17,231,624	2.714	15,376,339	2566	89%	114.20	1.11	2848
Poland	37,974,750	1.837	22,936,174	1737	60%	59.50	0.58	1004
Portugal	10,283,822	2.118	7,161,391	2003	70%	88.10	0.86	1715
Romania	19,472,545	1.788	11,447,407	1691	59%	55.70	0.54	915
Slovakia	5,446,771	1.756	3,144,709	1660	58%	84.20	0.82	1359
Slovenia	2,073,894	1.998	1,362,382	1889	66%	87.10	0.85	1599

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

Country	Population (2018)**	eHealth adoption (2018)***	# of primary health records	Estimated fixed cost of data permit authority (thousands) Euro	% health records/ population	PPP National currency units****	PPP National currency units/ Euro	Estimated cost of health data permit authority PPP National currency units/ Euro (thousands)
Spain	46,797,754	2.365	36,389,245	2236	78%	96.50	0.94	2097
Sweden	10,175,214	2.522	8,437,339	2385	83%	125.10	1.22	2899

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement between Estonia and Finland.

** Source: The World Bank website <https://data.worldbank.org/>

*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.

**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the aforementioned source and divided by the EU 2018 average of 102.9.

Source: Authors' elaboration

Table 39. Estimated variable costs for data permit authority

Country	PPP National currency units*	PPP National currency units/ Euro	Data permit for applicants in PPP National currency units/Euro		Fee per hour for data extraction, processing, and delivery in PPP National currency units/Euro		Use charge per month for remote access environment in PPP National currency units/Euro	
			Low range	High range	Low range	High range	Low range	High range
Austria	112.60	1.09	334	4004	100	153	250	614
Belgium	114.50	1.11	339	4071	102	156	254	625
Bulgaria	51.70	0.50	153	1838	46	70	115	282
Croatia	70.50	0.69	209	2507	63	96	157	385
Cyprus	90.40	0.88	268	3214	80	123	201	493
Czechia	73.90	0.72	219	2628	66	101	164	403
Denmark	141.90	1.38	420	5046	126	193	315	774
Estonia	83.40	0.81	247	2966	74	114	185	455
Finland	125.50	1.22	305	3659	91	140	229	562
France	113.80	1.11	337	4046	101	155	253	621
Germany	106.10	1.03	314	3773	94	145	236	579
Greece	86.60	0.84	257	3079	77	118	192	473
Hungary	65.90	0.64	195	2343	59	90	146	360
Ireland	134.10	1.30	397	4768	119	183	298	732
Italy	103.20	1.00	306	3670	92	141	229	563
Latvia	76.60	0.74	227	2724	68	104	170	418
Lithuania	67.40	0.66	200	2397	60	92	150	368
Luxembourg	130.00	1.26	385	4623	116	177	289	709
Malta	86.20	0.84	255	3065	77	117	192	470
Netherlands	114.20	1.11	338	4061	102	156	254	623
Poland	59.50	0.58	176	2116	53	81	132	325
Portugal	88.10	0.86	261	3133	78	120	196	481
Romania	55.70	0.54	165	1981	50	76	124	304

Country	PPP National currency units*	PPP National currency units/ Euro	Data permit for applicants in PPP National currency units/Euro		Fee per hour for data extraction, processing, and delivery in PPP National currency units/Euro		Use charge per month for remote access environment in PPP National currency units/Euro	
			Low range	High range	Low range	High range	Low range	High range
Slovakia	84.20	0.82	249	2994	75	115	187	459
Slovenia	87.10	0.85	258	3097	77	119	194	475
Spain	96.50	0.94	286	3431	86	132	214	527
Sweden	125.10	1.22	371	4448	111	171	278	683
United Kingdom	119.30	1.16	354	4242	106	163	265	651

* Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the aforementioned source and divided by the EU 2018 average of 102.9 to get the next column (PPP national currency units/euro).

Source: Authors' elaboration

4.1.2 Health data exchange for healthcare provision (primary purposes)

The use of health data for primary purpose in this report is defined as the data processing for the purposes of provision of health and social care by health and care providers to the patient concerned. This concerns data that is collected directly from a patient in the context of health and social care provision for the purpose of providing health or care services to that patient. This includes both in-person care and telecare using eHealth or mHealth tools (EC, 2020). It is important to note that the health system can be divided into different categories: healthcare (hospitals, general practitioners, labs, etc.), cure (elderly care) and public health (vaccinations, infectious diseases)

For primary use of health data, the focus will be on the access and exchange to health data by health providers and patients. Additionally, there are challenges in Europe for using health data, due to complexities caused by a myriad of languages, systems and structures, with challenging policy restrictions and technology considerations.¹⁴⁸ This section will focus on the outcomes found from the scoping review and will include practices of sharing health data, both cross-border and within Member States, as well as describe barriers and drivers of implementing interoperability and infrastructures to exchange this data.

Drivers and barriers for exchanging health data by stakeholders

Healthcare providers

Drivers for both cross-border and within-border. The capacity to share health data among care providers and patients is seen by many as an important aspect of improving patients' safety, reducing the number of avoidable mistakes, and improve the coordination and continuity of care (OECD 2017)¹⁴⁹. Exchanging health data between healthcare providers for the treatment of patients, helps facilitate coordinated patient care, enabling an organization to¹⁵⁰:

- Save time by minimizing readmissions
- Increase efficiency by moving away from paper and fax machines
- Save money by avoiding duplicate testing
- Provide clinical decision support tools to improve care and treatment
- Minimize medication and medical errors
- Engage consumers about their own personal health information
- Improve healthcare quality and outcomes.

For medical professionals, exchange of health data for primary purposes, specifically through platforms such as EHRs, facilitates easy access to a patient's records from a single electronic file. Using this patient record, doctors can read test results as patients' data are entered, including information even from remote hospitals.

Barriers. Technical barriers, such as setting up the infrastructure, ICT systems, and standardisation to enable stakeholders to share health data, are necessary to overcome. Stakeholders in Finland highlighted the challenge of bringing all levels of healthcare providers and government to a certain level of digitalisation – for example, the general practitioner has to

¹⁴⁸ [https://www.harmony-alliance.eu/en/news/wp7/new-imu-project-launched-ehden-european-health-data--evidence-network](https://www.harmony-alliance.eu/en/news/wp7/new-imu-project-launched-ehden-european-health-data-evidence-network)

¹⁴⁹ <https://www.oecd.org/health/health-systems/Economics-of-Patient-Safety-October-2020.pdf>

¹⁵⁰ <https://patagoniahealth.com/health-information-exchange-important-for-ehr/>

have the infrastructure to be digital as well as the municipality. This is an ongoing onboarding process that takes the commitment of the local and national governments. These challenges emerge even more so in the cross-border context in which certain dimensions are accentuated, such as language, legal, and differences in culture as well as common objectives and incentives.

As it has been mentioned in the EHDS inception impact assessment¹⁵¹, "*insufficient health data exchange negatively impacts on the provision of healthcare services (primary use of health data). The level of digitalisation at national level varies considerably and interoperability between healthcare providers remains limited. The eHealth Network – and its related IT infrastructure – has improved the cross-border exchange of health data for healthcare, such as patient summaries and e-prescriptions. However, among other challenges, its voluntary nature and the non-binding nature of its guidelines has affected the uptake and impact of its decisions*". Furthermore, "*there is fragmentation of digital standards and limited digital interoperability between healthcare systems. Recommendations on a European Electronic Health Record Exchange Format exist. Nevertheless, in practice they are not sufficiently applied, which reduces interoperability between systems and creates barriers in the Single Market. Few Member States apply the voluntary eHealth Network guidelines. The resulting market fragmentation hampers the free movement of digital health products and services with duplications and increased costs for healthcare systems, patients, researchers and public institutions. This fragmentation poses a significant challenge for businesses and enterprises and national healthcare systems when integrating innovations in healthcare*".

Patients

Citizens accessing personal data. Digitalisation and new technologies are offering a wealth of opportunities to collect, use and share health data more efficiently, such as to empower patients in managing their diseases, for research, and to improve the quality, safety, and efficiency of healthcare systems. But they pose new challenges for privacy and data security. However, there are also risks to be considered regarding digitalisation, such as data privacy or breaches, cybercrime, and the need to constantly adapt technology to the rapidly changing digital environment.

The legal environment of the eHealth Digital Service Infrastructure for the cross-border exchange of data supports cross-border healthcare and in so doing supports the continuity of care and the right of Europeans citizens to choose their healthcare provider in another Member States under certain conditions¹⁵². One of the ways to facilitate cross-border access is to increase and ease citizen access to and portability of their personal health data. More specifically, the right of access for citizens to their personal health data is defined in Article 15 GDPR and the right to portability is laid down in Article 20 GDPR.

Article 15 GDPR establishes the right for individuals to have access to their personal data, including concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided (recital 63 GDPR). While several rights of the data subject in respect of their personal data existed before the GDPR, the GDPR introduced the right of data portability. Data portability, as outlined in Article 20(1), implies a transmission from the controller's IT system to the systems of the data subject and allows the data subject to transmit their own data to another controller, without hindrance. There are limitations however, data

¹⁵¹ See Proposal for Regulation [tbc] on the European Health Data Space, digital health services and products and the use of new technologies, including artificial intelligence (AI) in health [https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares\(2020\)7907993](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares(2020)7907993)

¹⁵² https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co222_en.pdf

portability is conditional on Article 20(1)a and b which state that the right to portability applies when the processing is carried out by automated means and the legal basis for the processing is either:

- Consent (*one of the several possible legal bases as described in GDPR Article 6(1)(a), or as justification for processing of special categories of data under Article 9(2)(a) GDPR.*)
- Contractual necessity (*as also described in GDPR Article 6(1)(b)*)

It is also limited to the initial data provided by the data subject and not inferred data, such as results, which is a limitation that is not satisfactory in the context of health. As it has been mentioned in EHDS inception impact assessment¹⁵³, "*exercising access and control over their own health data is often difficult for patients. Electronic health records (EHRs) are not yet a reality across the whole EU, and many patients cannot easily access and use the information they contain, or transfer them between healthcare providers, including when they move across borders. This leads to duplication of efforts, inefficiencies, delays of treatment and higher costs for healthcare systems and patients. The interoperability of EHR and of mobile health tools is limited, meaning that this information cannot be easily used in the treatment of patients "*

Box 41. Article 20 Right to Data Portability

Article 20 (1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
- b) the processing is carried out by automated means.

Article 20 (2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Article 20 (3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 20 (4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Those provisions of the GDPR are applied in the context of cross-border healthcare covered by the 2011/24/EU Directive.

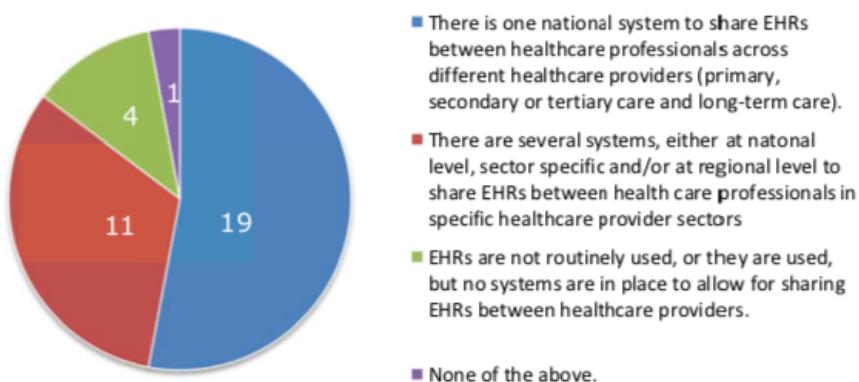
Electronic Health Records. Access to health data in electronic format and tools for portability at national level is currently associated with EHRs and Personal Health Records (PHRs). EHRs can be defined as a repository of digitally stored patient data (Flaumenhaft and Ben-Assuli 2018). A PHR is a similar electronic repository that is accessible directly by citizens, in some countries they are a subset of the EHR and may be seen by a healthcare professional, while in others they exist independently of the EHR. EHRs contain data that are originally collected for diagnosing and treating an individual patient but can also contribute significantly to research purposes,

¹⁵³ See Proposal for Regulation [tbc] on the European Health Data Space, digital health services and products and the use of new technologies, including artificial intelligence (AI) in health [https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares\(2020\)7907993](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares(2020)7907993)

public health purposes and monitoring of the healthcare system. This implies that the data stored in these repositories should be accessible and exchangeable among different administrative systems (EC, 2020). The way data are stored and coded may vary among the information systems that healthcare providers use. As a result, the availability and access and use of data vary across and within borders (OECD 2019). Furthermore, issues concerning consent for further use and accountability play an important role. Accountability should be demonstrated (who stores what and where for what purpose) in order to assess the legitimacy of the further processing of these data (Becker 2019, Goncalves-Ferreira 2018).

EHRs are a core building block for disease monitoring, surveillance, health- and health services research, as well as for the provision of care for individual patients (Blumenthal 2017, Verheij et al 2018). In almost all Member States there are ICT systems by which healthcare professionals can share the EHRs of individual patients with other healthcare professionals. Work done by DG SANTE project '*Assessment of the Member States' rules on health data in the light of GDPR 2019/2020*"', (EC, 2021) this sharing may be done with one national system or use several national, regional or sectoral systems: 18 out of the 27 Member States report having a national system through which data can be accessed and shared between health care professionals, while 11 report having more than one system, either sector specific or regional.

Figure 6. EHR sharing between health care professionals per Member State



Source: EC, 2021

Drivers for both cross-border and within-border. Benefits of patient access to their own health data are numerous such as less risk in medical situations due to swift access to patient medical records, higher engagement in their own health care, and increased mobility, among others. The main purpose of reinforcing control over their own health data (access and portability) is to facilitate treatment and healthcare. The benefits of citizens exchanging their personal health data and having better portability of their health data, in a cross-border context and within-border context, are numerous, including

- An increase in the feasibility to transmit data cross-borders to a health professional of their choice;
- Increase in understanding of patient care plans;
- Reduction in healthcare costs;
- Reduction in duplicative testing

The reduction in health care costs has been reported in several studies as well. In Canada for example, patients having access to their PHR generated value for Canadians and health systems

by increasing health system productivity and improving access to and quality of health care provided. As opportunities increased to interact and engage with health care providers via PHR functions, the marginal value generated by utilization of PHR functionalities also increased. Web-based prescription renewal generated the largest share of the total current value from the patient perspective. From the health systems perspective, Canadians' ability to view their information a secure personal web portal was the largest value share. It is cited that if PHRs were to be implemented with more integrated virtual care services, the value generated from populations with chronic illnesses, such as severe and persistent mental illness and diabetes, could amount to between \$800 million and \$1 billion (Canadian currency) per year across Canadian health systems (Hackett, 2019).

The GDPR defines a number of rights for individuals as concerns their personal data, also applicable to their health data, in particular:

- To access one's own personal data (Recital 63, Article 15)
- The right to data portability/to transmit data from one data controller to another (Article 20), though it has limitations that are relevant in the area of health;
- Right to rectification or erasure of data (Article 16)
- Right to erasure (right to be forgotten) (Article 17)
- Rights in case of data breach (Article 34)
- Right to lodge a complaint and to an effective judicial remedy, right to compensation (Articles 77, 79, 82)
- Right to be informed/transparency (Articles 12, 13 and 14)

Barriers for both cross-border and within-border. There are costs that are associated with patients/citizens' access to their own health data in an electronic format and the portability of such data, such as the concern of unauthorized access and dissemination of digitized healthcare information and the attendant risks to patient privacy. Another crucial cost is the introduction of IT solutions to facilitate the access to health data and the standardised and consistent entry of this data by healthcare professionals. The IT factors such as the interoperability and connectivity between systems must also be considered and should be implemented in ways that secure access solutions such as patient consent of registries for health access and healthcare provider access rights to registries. Another important IT factor is identification, currently different national eID schemes do not "travel" across borders seamlessly. Similarly, healthcare professionals have eID schemes in Member States that do not travel across borders either.

Breaches of patient information not only risk revealing patient data, but also result in remediation costs, penalties, or reputational damage. In addition, patients are unlikely to share their private information unless they are confident it will be handled securely (Anderson and Agarwal, 2011); such withholding may lead to poor health outcomes. Thus, healthcare security is closely related to the quality of care and deserves special attention. However, one of the ways to mitigate this risk is to increase tools that allow such access in electronic format, and to facilitate portability/their decision to share their data with other healthcare professionals.

In addition, digital access could exclude some parts of the population that do not have access to internet or do not have digital literacy (Merkel, 2020). The lack of digital literacy of an individual could prevent patients from accessing or understanding their health data. Furthermore, the progression of full patient access, as reported in the United States, to their EHR-tethered portal or personally controlled PHR has been slow historically. Some of the reasons were on the patient side and regarded privacy concerns that could be associated with full and open access to personal

medical information. This is due to the worry that this open access will lead to access of data by all kinds of healthcare professionals without the control or decision of individuals. On the provider's side, the reasons reported were that the technical nature of Web-based medical information could create a health literacy burden; and finally, concerns on the business side were that EHRs are not set up to support fully interoperable data exchange (Ford, 2016). A similar issue exists within the EU. Member States have different rules on the access to health data by healthcare professionals.

Barriers specific to cross-border. Feasibility and efficiency of systems to gain access to health data as well as facilitate data portability needs to be standardized and accelerated and created as common practice.

Furthermore, similar to the costs to provide cross-border services to exchange health data for healthcare providers, MS may be hesitant to spend the large, start-up costs of implementing cross-border interoperability due to the small numbers of patients seeking care abroad and the small impact the Directive had on patient mobility. It is important to note that in some Member States, the share of the population seeking healthcare across borders is quite significant.

Reports on the implementation of the Directive, such as an impact study performed in the Netherlands, Malta, Germany, Poland, Belgium, Finland, and Estonia in 2015, indicate that it had little impact on the numbers of patients seeking care abroad and that the impact of the directive varies between countries; the impact is smaller in countries where a large degree of adaptation had already taken place in response to the European Court of Justice Rulings (Azzopardi-Muscat, 2018). Therefore, MS may be lacking the incentive to fund or promote cross-border systems.

National data governance structures. With regard to how governments facilitate the sharing of health data, MS are organised differently and have different preferences¹⁵⁴. In Belgium, the government launched Vitalink, a government-developed digital platform used to facilitate the exchange of data at national level. Vitalink, can only be used to share data to and support primary healthcare. The benefits of having a national data governance system that shares and uses health data for primary purposes, include the following:

- Better and more efficient collaboration between different professional caregivers;
- More efficient care;
- Administrative simplification;
- Lower, long-term costs;
- And an increased involvement of the patient/client (De Backere, 2018).

Another health portal for health data launched by the Belgian government (in 2018) is "MaSanté – MijnGezondheid". Citizens can access their health data via their ID cards (eID). For Flemish patients/clients, De Backere (2018) stated that it was important that the data be stored by the government, rather than elsewhere, so it could guard the data against misuse and ensure the privacy of the end use rather than entrusting the data elsewhere.

Belgium also has health data platform called Healthdata.be, which currently focuses on simplifying the registration of health data by various healthcare providers with the goal of improving the quality of health research in the future. Healthdata.be collects data from more than 150 clinical registries in Belgium.

¹⁵⁴ See Study on Interoperability of Electronic Health Records in the EU at <https://digital-strategy.ec.europa.eu/en/library/interoperability-electronic-health-records-eu>.

Estonia is another example of a Member States that has prioritized the digitalisation and access of EHRs for both patients and healthcare providers; with the 2019 Annual European eHealth¹⁵⁵, identifying Estonia as the leading country for e-health innovation in Europe. Estonia developed a national system, e-Health Record, that integrates data from Estonia's different healthcare providers to create a common record that is available for online access by every patient. Functioning very much like a centralized, national database, the e-Health Record actually retrieves data as necessary from various providers, who may be using different systems, and presents it in a standard format via a national online portal, the e-Patient portal. It is also used by medical professionals, such as doctors, and allows for the benefit of easy access to a patient's records from a single electronic file. Using this patient record, doctors can read test results as they are entered, including image files such as X-rays even from remote hospitals. For assuring the integrity of retrieved electronic medical records as well as system access logs, the KSI blockchain technology is being used.¹⁵⁶

From the patient point of view, this national patient portal allows patients to do the following¹⁵⁷:

- See the prescribed and bought out medicines;
- View their medical data, i.e. medical records composed and entered into the health information system by the attending physicians, immunization data, dental care documents, examination results, health certificates and access to medical bills reimbursed by the Estonian Health Insurance Fund.¹⁵⁸
- Book and cancel doctor's appointments;
- Order reminders concerning booked doctor's appointments;
- Appoint representatives for the performance of activities (for instance for buying out prescription medicines);
- Inform simultaneously all medical institutions about changes in their contact details;
- Present declarations of intention concerning blood transfusions, organ donation or donation of one's body after death, to fill out a declaration of health, to enter and amend personal data, to appoint a contact person or representative;
- Check by name who and when the health data was viewed;
- And act on behalf of the persons who have appointed them as their representatives.

Current practices of cross-border exchanges of health data for primary purposes

Across the Member States of the Union there is a rich and diverse collection of health data and medical data, which are held in electronic form (European Medicines Agency, 2019). These electronic data can include electronic health records (EHRs), laboratory information with diagnostic data, prescribing data, dispensing data, data from disease registries, health determinant data, datasets from (non-)interventional studies and of civil registrations including cause of death. As further described in chapter 5. currently there are two electronic cross-border health services that are being introduced in EU countries (who have chosen to participate), ePrescription (and eDispensation) and Patient Summary.

¹⁵⁵ https://europe.himssMSAnalytics.org/sites/himssMSAnalytics_europe/files/eHealth%20TREND%20BAROMETER%20-%20HIMSSMS%20Analytics%20Annual%20European%20eHealth%20Survey%202019.pdf, conducted in collaboration between HIMSSMS (Healthcare Information and Management Systems Society) and McKinsey

¹⁵⁶ <https://e-estonia.com/solutions/healthcare/e-health-record/>

¹⁵⁷ <https://www.sm.ee/en/patients-portal-and-health-information-system>

¹⁵⁸ https://na.eventscloud.com/file_uploads/c5da2a5e465f932e6debe55020e70899_E-health-factsheet.pdf

1. **e-Prescription (and eDispensation)** allows EU citizens to obtain their medication in a pharmacy located in another EU country building on the online transfer of the electronic prescription from their country of residence where they are affiliated, to their country of travel.
2. **Patient Summary** provides information on important health related aspects as part of a larger collection of health data called electronic Health Record. The digital Patient Summary is meant to provide doctors with essential information in their own language concerning the patient, when the patient comes from another EU country and there may be a linguistic barrier.

The eHealth Digital Service Infrastructure (**MyHealth@EU**) is the backbone system for facilitating these cross-border exchanges of health data. The European Commission and Member States are providing common ICT infrastructure guidelines, including terminology and interoperability to Member States. This platform is supported by the Commission and provides a common network and infrastructure to connect participating Member States' national contact points for eHealth.

Up to date, e-Prescription and Patient Summary involving cross-border data exchanges through MyHealth@EU are being gradually introduced in 25 EU Member States, of which only 7 have already introduced it as of today¹⁵⁹: The exchange of ePrescriptions and Patient Summaries through MyHealth@EU is open to all the Member States on a voluntary basis, but due to varying levels of availability of eHealth services at national levels, progress across the Member States as concerns adoption of e-Prescription and the Patient Summaries varies considerably. This clearly inhibits the possibility for cross-border exchange of patient data in the EU.

The exchange of health data across borders takes place in many instances already. Often, this takes the form of paper, DVD or fax exchanges. One example where two governments are working on digital exchange of health data is the Maastricht-Aachen university hospitals in Netherlands and Germany. They exchange health data connecting digital platforms from the radiology societies of Netherlands and Germany. Another example is the Benelux initiative, where they explore the digital exchange of health data, as decided by the Benelux in 2020.

Although the cross-border exchange of data between Member States is still far from reaching full interoperability, some Member States have formed legal agreements between each other to accelerate cross-border mobility for their citizens.

An example of this is the interoperability of ePrescriptions in **Finland and Estonia** through MyHealth@EU. Since 2019, Finnish patients can retrieve medicine in Estonia even though it was prescribed electronically by their doctor in Finland. Among other countries, Finland and Estonia signed the "*Agreement between national authorities or national organisations responsible for national contact points for eHealth on the criteria required for the participation in cross-border eHealth Information Services*" (Agreement) and provided legal bases in their national laws for exchanging ePrescriptions (eHDSI Legal Report, 2019)¹⁶⁰. As of 2020, Estonia citizens can also purchase medicine in Finland, using an ePrescription from Estonia. The restrictions in order to safeguard pharmaceutical safety are to dispense the medication according to the legislation of the country where it is getting dispensed, not the country where the treatment was prescribed. The agreement between Estonia and Finland is seeing benefits with patients, with a cited of about 20 pharmaceuticals dispensed a day (prior to COVID-19 cross-border restrictions) in

¹⁵⁹ https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en

¹⁶⁰ https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co22

Estonia with Finnish prescriptions. Now other Member States including Croatia, Portugal, Sweden, Poland, Ireland, and the Czech Republic, are planning to deploy the service.

With respect to exchanging health data for rare diseases, the European Reference Networks (ERNs), which is a network separate from MyHealth@EU to support patients with a complex rare disease and conditions, developed a Clinical Patient Management System (CPMS) which was successfully adapted to provide a platform for secure and GDPR-compliant exchange of patient data across borders and between hospitals in a Member State¹⁶¹. ERN registries contain data at an EU level and even data from non-EU/EEA countries. Through the CPMS system and the ERN registries, ERNs are an important example of health data processing for both primary and secondary use for rare diseases across borders.

4.1.3 Health data access for research, innovation, policy-making and regulatory decision (secondary purposes)

The use of health data for secondary purposes includes the usage of health data that was initially collected in the context of providing care, but that is used to drive innovation and research as well to improve and support the efficient functioning of healthcare systems. In line with the EC (2020) study "Assessment of the EU Member States' rules on health data in the light of the GDPR", the re-use that stakeholders can give to health data would typically consist in; (I) **data processing for wider public health purposes** including planning, management, administration and improvement of healthcare systems, prevention or control of communicable diseases, protection against serious threats to health and ensuring high standards of quality and safety of healthcare and of medical products and medical devices, and (II) **data processing for scientific or historical research** by both public and private sector organisations, including the pharmaceutical and medical technology industries and insurance providers.

Important stakeholders re-using health data for secondary purposes include public entities such as national health systems statutory payers (public bodies of health insurers), public research entities (including universities, public health laboratories), regulators such as medicines agencies and notified bodies as well as the industry (including large and small pharmaceutical and medical technology companies, insurance and financial services sector companies, the social media and consumer electronics actors, and the emerging AI industry).

The drivers and barriers of access to health data by researchers, policy makers, and regulators are outlined below as well as business to business access, business to government access (B2G), government to business access (G2B).

Drivers and barriers for cross-border and within-border access by stakeholders

Researchers

Drivers. As it has been estimated in section 0, the potential value of health data is promising. Access to health data, when legal and ethical usage of data is ensured, can be used to provide researchers with crucial information necessary for the improvement and development of therapies and treatments, such as pharmaceutical drugs or population-level studies across Europe. Nowadays, it is very difficult to conduct scientific research because health data is not openly shared or comparable among researchers across Europe. Since allowing access to high-quality, interoperable health data sets has a number of benefits for stakeholders such as researchers, the European Commission identified as a key priority the development of a European Health Data Space (EHDS).

¹⁶¹ https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20200603_sr_en.pdf

One of the benefits reported in the literature is that access to health data increased feasibility and effort to gather comprehensive data to accurately assess the new therapies (Auffray, 2016). This also reduces costs and can broaden the scope of the studies. In fields where large sets of patient data are required, such as in genomics or epidemiology, researchers would greatly benefit from a wider access to information.

The availability of health data for research can be particularly helpful in cases of rare diseases, in which there is a lack of data; researchers have a large gap in the understanding of these diseases and data interoperability can help facilitate the transfer of knowledge. Rare diseases have been addressed by the Commission through the creation of European Reference Networks on the basis of Article 12 of Directive 2011/24/EU, which are then further supported by *Article 13 of the 2011/24/EU Directive*, which calls for the cooperation of diagnosis and treatment capacity through different tools available at Union level. These tools are available through the European Platform on Rare Disease Registration (EU RD Platform), concerning a central metadata repository, the European Directory of Registries and a pseudonymisation toolkit.

Limiting access for researchers has been cited as a significant factor of inhibiting breakthroughs and accurate conclusions in medicine. One of these examples is the U.S. Medicare & Medicaid system which contains high quality, comprehensive, national data sets which have strict limits on who can access or share them. It is argued that too much limitation can "distort the pool of potential researchers, the types of research that might be conducted, and potentially, the conclusions that could be legitimately drawn from that research" (Berger, 2015). Following on this concept, the United States established the Cures Act in 2016 with the purpose of easing access for researchers to health data by allowing researchers to waive the requirement for informed consent in the cases where clinical testing of drugs or devices "poses no more than minimal risk" and "includes appropriate safeguards to protect the rights, safety, and welfare of the human subject."¹⁶² However, having a lower barrier to acquire patient health data comes at the cost of many concerns over data protections that need to be taken into account by policy makers. In the US, the approach to data protection and security differs from the EU, as in the area of health this is regulated with the HIPAA regulation. One of the strengths of HIPAA in terms of data is the clear definition of what constitutes health data or "Protected Health Information" (PHI). The regulation also includes medical scans and EHRs, and counts with a specific "privacy rule" that covers all applicable organisations. This privacy rule aims at making sure patient data stays under the control of the patient through a set of patient rights on the use of data, and also limiting the ways patient data can be used. It is worth mentioning that in the EU, the GDPR provides a comprehensive framework laying down rules to ensure appropriate level of protection of personal data.

Additionally, patient access to their own health data, has also been associated with increased access to health data by other stakeholders, such as researchers and policymakers, based on individuals' control over their own data. When surveyed, majority of citizens would give consent to share their health data to researchers as long as their data is being used ethically and not for commercial reasons. When access may be restricted to governmental-sponsored data sets, some reports argue that the way to reduce limitations to data access is to give patients broader rights to control the use of their data. Therefore, patients themselves could facilitate other stakeholders' access to data, as long as there are interoperable, efficient systems for patients to give consent (Berger, 2015). This concept could be to support "data altruism" platforms in which individuals can consent to "donate" their data for wider public goods.

¹⁶² "21st Century Cures Act", PUBLIC LAW 114–255—DEC. 13, 2016

Barriers. The highest cost of not facilitating access to health data by researchers are in terms of health outcomes and the quality of life of patients. One of the most important barriers for scaling-up not only for integrated care but also research across Europe remains the deployment of interoperable digital technologies, including the exchange of EHRs across-borders. Although, this could be considered a prerequisite, this will not be a guarantee of EU wide health data sharing for research purposes. Low levels of use and achieved interoperability will impact directly projects, such as the building of the European 1+ Million Genomes (1+MG) initiative¹⁶³. If EHRs are not interoperable within a Member State, let alone across borders, such requirements and initiatives for linking data will remain a very scientific enterprise as opposed to real implementation within mature infrastructures. Another barrier is the lack of public understanding and therefore trust, for uses of data that are not directly applicable to the individual and performed by organisations who seem less familiar within the health ecosystem (iHD & Digital Health Society, 2021). Apart from lack of public understanding and interoperability, lack of access is another barrier; with researchers often facing complex and difficult-to-understand rules on accessing health data¹⁶⁴.

Regulators and Policymakers

Governments have been moving away from the digitalisation of documents, processes and decision-making towards a new model that involves citizens in the co-production and information sharing¹⁶⁵. The sharing and use of health data are crucial when dealing with public health threats and management of public health systems.

Drivers. Access for policy makers and regulators can result in data-enabled public health prevention and promotion strategies. Examples can include (i) large and integrated environmental, genetic and socio-economic datasets could enable better prediction of risk factors for disease; (ii) data on health apps and portable devices could enable citizen empowerment and proactive behaviours in maintaining good health; (iii) computer algorithms and predictive analytics could assist in disease screening and early diagnosis (Marjanovic et. al. 2017). Regulators should use anonymised data whenever possible. However, in certain circumstances these agencies, such as the European Medicine Agency (EMA), have access to pseudonymised data such as clinical reports submitted for marketing authorisation or post authorisation procedures. However, these reports cannot be published as they are not anonymised.

Furthermore, as seen in the current situation of the COVID-19 pandemic, access to health data can better prepare countries to deal with threats to public health, such as disease outbreaks.

Barriers. Barriers to the re-use of health data for regulators and policy makers are numerous. The data is often collected for healthcare purposes, which means the data is not necessarily fit for other purposes. Also, data access is restricted according to legal and ethical grounds. Furthermore, data are collected using certain standards, these do not translate easily to other purposes. Additionally, fear of data misuse, including fears that information will be used in some way to disadvantage or discriminate against individuals or minority sub-populations, must also

¹⁶³ <https://digital-strategy.ec.europa.eu/en/policies/1-million-genomes>

¹⁶⁴ <https://www.digitaleurope.org/resources/data-flows-and-the-digital-decade/>

¹⁶⁵ Bani, M.; & De Paoli, S. (2020) "Ideas for a new civic reputation system for the rising of digital civics: digital badges and their role in democratic process". *ECEG2013–13th European Conference on eGovernment: ECEG*.

be addressed by such bodies (iHD & Digital Health Society, 2021). In addition, as mentioned in the EHDS inception impact assessment: ¹⁶⁶

- *The collection, access, storage, use and re-use of personal health data in healthcare poses specific challenges. The General Data Protection Regulation (GDPR) sets out the EU data protection rules. However, Member States may further specify some aspects in specific areas, such as health data, which they have done to a large extent. As a result, the processing of personal health data in Member States is fragmented, leading to obstacles and to limited access of researchers and public institutions, that in turn reduces the EU competitiveness and innovation potential at a global level.*
- *MS have different approaches for access to and sharing of health data. Some Member States have set up national bodies facilitating access to health data; however, such bodies do not exist in all Member States. Limited cooperation, governance and IT infrastructure at EU level hinders health data access for researchers, public institutions and regulatory bodies. The horizontal proposal on the Data Governance Act which lays down a governance framework for the common European data spaces can address these limitations only partially due to the specificity of health data.*
- *Evidence-based policy-making and regulatory action would benefit from additional access to timely, accurate, representative data of high quality held by public and private organisations (e.g. private healthcare providers). The re-use of health data held in cross-border databases is difficult due to the different applications of the GDPR in the areas of health and research in the Member States. This limits the sharing of privately and publicly held health data and genetic data (1+ Million Genomes initiative) with researchers, innovators, public bodies or regulators.*

Drivers and barriers for business and commercial access for research and innovation

Drivers. Benefits of commercial access for research and innovation can include improved health outcomes based off accelerated innovation in health research. Ultimately, limiting access to businesses also means limiting research and the improvements for health outcomes that could be achieved. When considering business access to government health data for research and innovation, there are benefits to consider. "Accessing data held in public authorities' data spaces is critical for research and development, and also to monitor and to evaluate the outcomes or health economic efficiencies of medicines in real life settings (after marketing authorization). Government official sources, when regulated to provide objectively measured data, are reliable and trustworthy sources of data. They also can provide clear traceability, allowing a population-based analysis of health data."¹⁶⁷

Particularly in companies performing pharmacological research, access to diverse and larger amounts of real world data, coupled with more granular information on patient profiles, could facilitate quicker and more rigorous learning about how drug safety relates to particular patient groups over time, including in the context of co-morbidities (Marjanovic, 2017).

Collaborations between businesses, to exchange data, can ultimately accelerate research and the ability to improve outcomes for patients. Additionally, growing costs in research and development along with the availability of technology are forcing disruptions in the approach to

¹⁶⁶ See Proposal for Regulation [tbc] on the European Health Data Space, digital health services and products and the use of new technologies, including artificial intelligence (AI) in health [https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares\(2020\)7907993](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares(2020)7907993)

¹⁶⁷ Statement from Sanofi from the targeted consultation activity performed for this study.

regulatory submissions and approval. A driver for businesses to collaborate are the potential cost-savings in research in development.

Barriers.

Business to business access to health data is not particularly well-regarded by the public. As reported by Mounton (2018), there is public distrust towards the use of data sharing for commercial reasons. One of the fears is data is shared based on the grounds of social benefits, but if patients do not see the benefits, this could foster distrust towards healthcare professionals, the public healthcare system in general, thus reducing the expected social benefits. It can also be argued that the increasing computerisation and centralisation of health data collection could further exacerbate the monitoring of individuals, increasing the chances of potential abuse (Belli, 2017).

From the business side, businesses may also be hesitant to share health data due to the risk of non-compliance with GDPR and data breaches, since they can only share personal data if they have a valid legal basis to do so. If the data security is compromised, organizations could face a damage to their reputation or loss of competitive advantage (Mazor, 2017).

Business to Government. There is still much development to be made in the creation of technologies that securely transfer private sector data to public sector. The exchange of B2G data is currently not happening at a large scale because the value of data as an asset is not yet fully recognised, and public bodies frequently lack the know-how to identify valuable datasets as well as the capacity to process them. In addition, there are currently not enough incentives for businesses to share data with the public sector for the common good. There are also a number of other barriers, including a lack of professionals in the field, differences in legalisation between Member States, data protection and security issues, ethical questions and the limited interoperability of datasets, amongst others. As a result, B2G data sharing can be a lengthy, uncertain process¹⁶⁸.

Another inhibitor of implementing B2G systems are high costs. The European Commission's High-Level Expert Group on Business-to-Government Data Sharing recommends that through Horizon Europe and Digital Europe Programme, the Commission funds the development and deployment of technologies needed to implement B2G data sharing at scale and in a responsible and sustainable way. Specifically, the Commission should fund proposals on privacy-preserving technologies, security technologies and access control technologies.¹⁶⁹ Also due to legal obstacles, B2G exchanges normally comprise of short-term projects, which slow the full benefits of these partnerships.

Government to Business. With regard to government to business access to health data, there are a number of concerns surrounding this practice. When considering, for example, the French Data Hub, there has been criticism from the French data protection authority, particularly regarding the protection of anonymity and the concern that the purpose of research may be too broadly described in the law and critics argue these two factors could cause an exploitation of French citizens' personal health data (AlgorithmWatch.Org, 2020). The inhibitors are reflected in the concerns for the French Health Data Hub; are there enough legal protections in place to prevent the data from being exploited for commercial reasons in the future? Should "public interest" be defined further by law? For what kind of purposes should health data be made accessible for secondary use? Would it be possible and socially acceptable to make available

¹⁶⁸ <https://ec.europa.eu/digital-single-market/en/faq/faqs-business-government-data-sharing>

¹⁶⁹ Towards a European strategy on business-to-government data sharing for the public interest , Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

health data for non-public interest purposes, such as commercial use, and under what conditions? As another similar example of existing practice in the EU, it is relevant to highlight the example of Findex, a Health and Social Data Permit Authority in Finland, which facilitates access to health and social data in a secure manner¹⁷⁰. Findex facilitates access to health data for secondary purposes, including research and innovation, through **The Act on the Secondary Use of Health and Social Data (552/2019)**, which provides a legal basis on the use of health and social data for secondary purposes. Under this act, research based on register data can be carried out without separate consent. It is important to note that this health information cannot be used for marketing or the definition of individual commercial services, such as insurance premiums.

Current practices for national health data exchange for secondary purposes

National data governance structures

There exist different governance structures and strategies for managing health data in the Member States, with a particular focus on re-using data for research purposes. These include national agencies or bodies authorized to grant permits for the use of data already collected for another specific purpose, as well as any other mechanisms for providing access to health data for research and public policy purposes, including by means of initiatives to further enhance data altruism (EC, 2021).

On this section we outline thirteen data governance bodies at a Member States level as well as one in the UK, identified in the EC (2021) study "Assessment of the EU Member States' rules on health data in the light of GDPR". Even though the list is not exhaustive, it describes the main bodies that currently have a central role for providing access to health data for research, often existing in parallel to other bodies and data controllers that are in place. **The list shows that in some countries governance is arranged in more institutionalised public formats while other Member States rely more on within private sector governance.**

Bulgaria. The National Centre of Public Health and Analyses (NCPHA) provides statistical information following the Health Act (HA) and the Personal Data Protection Act. A written application can be made to provide access to data by the NCPHP, but to date this is limited to public information.

Cyprus. The Ministry of Health and the National Bioethics Committee evaluate research applications made. The National Bioethics Committee consists of three Review Bioethics Committees, that review protocols relating to; (I) biomedical research on human beings and their biological substances, (II) clinical trials on Medicinal Products for human use, and (III) Medical devices applied on human beings. Even for pseudonymised data, the National Bioethics Committee needs to provide the researcher with a decision whether there is a need for full application of ethics. Researchers need to attach the decision of the National Bioethics Committee to their application to the Minister of Health. Application fee is 50 Euro. Other than this, there is no fee payable.

Denmark. The two national data governance bodies that host health data are: Statistics Denmark (storing data about the wider Danish population) and the Danish Health Data Authority (hosting disease registers and databases with health-related information). Researchers can apply for access to data locally with data custodians, or for the whole country either through the Researcher Service (Forsker-service) xrat Serum Institute (when it is health data only) and through Statistics Denmark, if the researcher wants to combine health data with other data

¹⁷⁰ <https://www.findex.fi/>

types. Denmark has very comprehensive national registries, which is unique in a global context. Stakeholders consulted, reported the importance of maintaining trust of citizens through high security systems and strict regulation around the use of health data.

Finland. Findata is an independent central agency which operates under the performance management of the Ministry of Social Affairs and Health (see also section 7.8 for a detailed description). Findata provides access to, develops and guides Findata's operations. The Data Protection Ombudsman, Parliamentary Ombudsman and Valvira¹ supervise the operations of Findata and compliance with the Secondary Use Act.

Permits can be obtained for the secondary use of personal data. For statistical data, a data request can be done. Findata issues permits for obtaining data in cases involving secondary use of health and social data, and combining data from registers of multiple controllers or obtaining data from private social welfare and health care service providers. Access is granted via a remote access environment (unless transferring of data is absolute necessary). Fees apply for the application procedure, the costs of data controllers to extract the data, working hours of Findata personnel for processing the data and for the remote access environment. Data requests are currently possible only with a Finnish personal identity code through Suomi.fi identification.

France. The Health Data Hub builds on previous initiatives and is set up as the single-entry point for health data access in France providing access for all researchers to data currently stored in the Health Data Hub. It is also responsible for health data access governance as it hosts the secretariat of the CESREES, the ethical and scientific committee for health research, studies and evaluations, which evaluates requests for access to the data catalogue. The Health Data Hub is both affiliated with the Ministry of Solidarity and Health, and with the Ministry of Research. The missions of the Health Data Hub are determined through Article L. 1462-1 of the Public Health Code. The health data platform, with its governance set up by decree, is composed of 56 entities that represent, among others, the State, organizations ensuring representation of patients and users of the health system, producers of health data, public and private users of health data, including health research organizations.

Germany. The Research Data Center DaTraV at BfArM (Federal Institute for Drugs and Medical Devices), supported by the Federal Ministry of Health is currently being set up. Researchers can apply to access data that BfArM holds, covering records of citizens with statutory health insurance. As of 2023 it is expected to provide access to EHR data for which patients will be able to grant access to.

In addition, the Federal Ministry of Education and Research is setting up a National Research Data Infrastructure (NFDI) for the entire research landscape. The NFDI will act as national repository and systematically manage scientific and research data. It provides long-term data storage, backup and accessibility, nationally and internationally. Using a budget of 90 million EUR from 2019-2028, the NFDI will bring stakeholders together in coordinated consortia tasked with providing science-driven data services to research communities. The first consortia are starting in October 2020, including for health data a) a National Research Data Infrastructure for Personal Health Data, NFDI4Health and b) a German Human Genome-Phenome Archive (GHGA).

Third, is the Medical Informatics Initiative (MII) as set up by university medical sites. MII creates a harmonized framework for nationwide access to the exchange and use of patient data and biomaterials for medical research. Participating sites have agreed on a comprehensive model of usage regulation for the exchange of patient data, biomaterials and analysis methods and routines, among others providing uniform application procedures and transfer points at all participating locations, which guarantee secure data transfer. The German Medical Informatics

received 160 million euros of investment from the Federal Ministry through 2021 to develop strategies for interoperability such as standardized templates for patient consent, data management, data protection, rules for data use and access, among others¹⁷¹. The integration of data from university hospitals into a usable and shareable system was cited as the first step in the direction of facilitating the use for researchers in Germany. This system remains in the federated system and was implemented with the goal advancing breakthroughs in healthcare by facilitating the access for researchers on crucial information. There is no information about the intention of EU wide research data sharing of the German national health data.

Greece. In Greece, IDIKA S.A. (e-Government Center for Social Security Services) is an agency supervised by the Greek Ministry of Labour, Social Security & Social Solidarity, responsible for access to health insurance claims data, prescribing and dispensing data, and disease registry data. Information is accessible for all types of organisations. Law 4600/2019 Article 84 (11) states that the agency is allowed to publish or grant, on a subscription or special fee, statistical data, from which the data subjects can no longer be identified and which come from the operation of the archiving system of the Individual Electronic Health Record. The data access organization is financed by the government.

Ireland. The NREC COVID-19 (National Research Ethics Committee (NREC) for COVID-19) is a temporary committee to deliver an expedited process for review for all COVID-19-related research studies. It is installed as part of Ireland's response to the COVID-19 pandemic. In accordance with the WHO roadmap for R&D the Minister for Health established the National Research Ethics Committee (NREC) for COVID-19 to deliver an expedited process for review for all COVID-19 related research studies.

The temporary NREC COVID-19 is designed to include structured and coordinated interaction with other bodies involved in regulation of health research including the Health Products Regulatory Authority (HPRA) and the Health Research Consent Declaration Committee (HRCDC). In this way, researchers and sponsors can expect to receive all the necessary decisions from appropriate parties within the same expedited timelines. The ambition of the NREC COVID-19 is to relay decisions back to researchers within 7 days of confirmation of a validated application.

An application form must be completed which includes review and feedback on the study by the relevant local Data Protection Officer. A data impact assessment must be included where necessary. No fee is applicable, and once in receipt of approval from NREC COVID-19 the study can proceed.

Latvia. The Center for Disease Prevention and Control (SPKC) has a delegated function to issue a permit for the use of patient data recorded in medical documents in a specific study. The examination of the application and the decision on the issuance of the permit shall be performed by a specially established SPKC commission.

Pursuant to a four-party cooperation agreement (between the Center for Disease Prevention and Control, the National Health Service, the Emergency Medical Service and the Health Inspectorate) on the establishment of a health care quality and efficiency monitoring system, a database has been created linking data from the above institutions.

Provision of statistical and research data from the information systems of the Center for Disease Prevention and Control is free of charge, except in the case that additional data processing or

¹⁷¹ Medical Informatics Initiative Germany. (2018, July 5). BMBF provides funding for the Medical Informatics Initiative. Retrieved October, 2020, from <https://www.medizininformatik-initiative.de/en/bmbf-provides-funding-medical-informatics-initiativ>

special data selection techniques are required to prepare the requested data have to be performed on the data by SPKC.

Malta. The Ministry of Health, Department of Health Information and Research (DHIR) hosts health data available for research purposes, this as part of an e-health network of multiple data controllers. Data concern primary and hospital care electronic health records, disease registries and linked health, social and environmental data. There are two different application procedures, one for aggregated data and one for record level data. For the latter case, the researcher should sign a document explaining the policy for requests of record level data files and fill out the request for record level data form. Before person-identifiable data can be released, prior approval for the data must be obtained from the relevant authorities and the same applies to ethics approval/clearance (when applicable, as determined by the Data Controller).

Netherlands. Statistics Netherland (CBS) can be seen as a data access body though CBS has not been set-up as a data access body for health care data (see also section 7.8 for a detailed description). CBS collects individual level data from a variety of sources for its statistical output or contribution to Eurostat. The Act on CBS allows researchers to use the CBS microdata in a secure environment. This can also be done by remote access and researchers are even allowed to bring their own data, provided that they have a legal ground to process and combine the data and may combine those with CBS data including the data about causes of death. There is strict output control and only the fully anonymised data can be exported. Though there is control by CBS on the type of research being carried out, this control cannot count as ethical review of the research.

CBS is an independent administrative body according to Dutch law. It is funded by Dutch government. Researchers who want to make use of the microdata pay a fee for setting up the remote access facility and additional costs of CBS for running the analyses.

Apart from CBS the Health Research Infrastructure (HealthRI) is an important organisation in the Netherlands to support secondary use of health data for research. They receive funding from universities and the Dutch MoH and provide the research tools and expertise to support secondary use of health data.

Portugal. The SPMS - Shared Services of Ministry of Health, Portugal is a public enterprise created in 2010, with the aim to provide shared services – in the areas of purchasing and logistics, financial services, human resources, information and communications systems and technologies – to organisations operating specifically in the area of health, in order to “centralise, optimise and rationalise” the procurement of goods and services within the National Health Service (NHS). It has the status of National eHealth Agency in Portugal and manages information systems that support the daily activity of health professionals in the Portuguese NHS.

At SPMS national and institutional level, a Coordination group for “Secondary use of health data” requests has been created to manage requests of health data for secondary use purposes. This group is multidisciplinary (data analysts, health professionals and legal experts) and reviews requests to be submitted to the Data Protection Officer, ensuring a single point of entry and smooth path for researchers from request to data sharing. It manages and oversees the entire process, from request to data sharing.

Slovakia. The National Centre of Health Information (NCHI) operates the national EHR system and certain health registries. It hosts the data and researchers can submit a request for NCHI to prepare datasets based on data in its registries (a project submission is necessary in such cases). Financing shall be required and NCHI usually will require to be co-researcher.

United Kingdom. A national institute for health data in England, Wales, Scotland and Northern Ireland has been created recently, called Health Data Research UK (HDR UK). It works with a wide range of health data from the NHS, universities, research institutes and charities, and increasingly from wearables, and private companies. HDR UK is a federated institute, benefiting from teams and physical offices located across the four nations of the UK. It is an independent, non-profit organisation supported by 10 funders (the British Heart Foundation, Chief Scientists Office, Health and Care Research Wales, Health & Social Care R&D Northern Ireland, Engineering and Physical Sciences Research Council, Economic and Social Research Council, Medical Research Council, National Institute for Health Research, Wellcome, and UK Research and Innovation).

Data can be accessed via the Health Data Research Innovation Gateway. This portal provides a common entry point to discover and request access to UK health datasets. Detailed information about the datasets, made available by members of the UK Health Data Research Alliance.

Before a researcher is granted access, their study is usually assessed by an independent review committee or other decision-making group, who ensure that the reason for using the data is appropriate.

Access for research and innovation

However, many Member States do have government-funded platforms that allow access to health data for research purposes, as shown in Table 40. In some cases, such as the data controller provides direct access with engagement of an ethics committee or data permit authority and other times it does not (e.g. Slovenia). To view the specific conditions under which researchers can access health data, see the country fiches in the digital health country factsheet document that was submitted with this report.

Majority of Member States do not have programs that incentivise the access of government health data by businesses. However, there are some exceptions. Business Finland¹⁷² is a public organisation, directed by the Finnish Ministry of Employment and the Economy, that supports research and development by incentivising health data access between businesses. The French Health Data Hub facilitates the reuse of health data for research projects by both public organisation and private entities. Thus far the HDH has set up several partnerships and projects to incentivise health data access between businesses.

¹⁷² <https://www.businessfinland.fi/en>

Table 40. Government-funded platforms in which researchers can access health data for research purposes

	Yes/Planned*/No		Yes/Planned*/No
Austria	Yes	Italy	Yes
Belgium	Yes	Latvia	Yes
Bulgaria	Yes	Lithuania	Yes
Croatia	Yes	Luxembourg	No
Cyprus	No	Malta	Yes
Czechia	No	Netherlands	No
Denmark	Yes	Poland	No
Estonia	Yes	Portugal	Yes
Finland	Yes	Romania	No
France	Yes	Slovakia	Yes
Germany	Yes	Slovenia	Yes
Greece	No	Spain	Yes
Hungary	Yes	Sweden	Yes
Ireland	Yes		

Source: Author's elaboration

Current practices for cross-border exchange for secondary purposes

EU cross-border exchange

A Joint Action¹⁷³ was initiated by the Commission in 2020 to support Member States with the aim to address differences in national GDPR implementation in the health sector and to support the development of a European Health Data Space and the re-use of health data for secondary purposes. Recently, also new actors at national level, such as data permit authorities or institutions dealing with secondary use of health data (e.g. Findata, French Data Hub etc.) have been set up by the Member States to support the processing of health data for secondary use in compliance with the GDPR.

In **the EU**, a multi-stakeholder collaboration has started, with the goal of compiling clinical data and developing a system to **facilitate health research** in the region. This collaboration, funded through the Innovative Medicine Initiative¹⁷⁴ (IMI) and called the European Health Data & Evidence Network (EHDEN), began in 2018 and is a 5-year project to build a data network to perform fast, scalable and highly reproducible research. According to their website, the goal is to standardise 100 million patient records across Europe from different geographic areas and data source types, such as hospital data, registries and population databases.¹⁷⁵

1+MG is another example of an initiative that through cross-border data access, has the potential to improve disease prevention, allow for more personalised treatments and provide new impactful research. Furthermore, the Beyond 1 Million Genomes (B1MG) is a Horizon 2020

¹⁷³ https://ec.europa.eu/chafea/health/funding/joint-actions/documents/ja-european-health-data-space-2020_en.pdf

¹⁷⁴ <https://www.imi.europa.eu/>

¹⁷⁵ <https://www.harmony-alliance.eu/en/news/wp7/new-imu-project-launched-ehden-european-health-data-evidence-network>

project that provides coordination and support to 1+MG Initiative to create a network of genetic and clinical data across Europe. 1+MG has a long-term goal of sharing data beyond 2022 and currently has a commitment from 23 European countries to give cross-border access to one million sequenced genomes by 2022.

The Directorate-General for Research and Innovation of the European Commission funds, through grants, many European health data research infrastructures for secondary uses of health data across the EU. Some of these research infrastructures and their corresponding costs are shown in Table 41.

Table 41. Examples of EU health infrastructures

Project name	Description	EU contribution	Overall budget
Population Health Information Research Infrastructure (PHIRI)	Aims to set up a research infrastructure that will facilitate and generate the best available evidence for research to assess the direct and indirect impacts of COVID-19 on population well-being, disease and mortality.	€4 890 327	€4 999 577
Innovative, Non-invasive and Fully Acceptable Exploration Technologies (InfAct)	Aims to unite stakeholders of Europe's future raw materials security in its consortium and activities via effective engagement of civil society, state, research, and industry.	€5 624 029	€5 624 029
ImpleMentAll	Aims to develop, apply, and evaluate tailored implementation strategies in the context of on-going eHealth implementation initiatives in the EU and beyond.	€5 999 170	€7 071 638
European Open Science Cloud-Life (EOSC-Life)	Aims to create an open, digital and collaborative space for digital biology in Europe.	€26 145 996	€26 145 996
European Joint Programme on Rare Diseases (EJP-RD)	Aims to develop a sustainable ecosystem to improve the lives of rare disease patients.	€55 073 831	€100 362 308
HealthyCloud	Defining the strategic agenda for the European Health Research and Innovation Cloud	N/A	N/A

Source: Authors' elaboration

IMI, the innovative medicines initiative, is an important public-private partnership for advancing research in health care. The goal of IMI, particularly in its second phase (IMI2, 2014-2020) is to develop next generation vaccines, medicines and treatments, such as new antibiotics. It has a budget of €5.3 billion, with 169 current projects and 7,000 project outputs.

An example of how the access and exchange of health data is used for **cross-border regulatory** purposes is through the ECDC's molecular surveillance of antimicrobial resistant pathogens (CCRE survey)¹⁷⁶, the goal of which was to reduce the risk of infectious diseases by monitoring

¹⁷⁶ https://www.ecdc.europa.eu/sites/portal/files/documents/Protocol-genomic-surveillance-resistant-Enterobacteriaceae-v2_0.pdf

multidrug-resistance bacteria. Prior to being transferred to the ECDC, patient data was collected by national institutions in participating countries from the European Union (EU), European Economic Area (EEA), EU candidate and potential candidate countries and pseudonymised for the CCRE survey to maintain patient confidentiality¹⁷⁷. Recipients of pseudonymised patient data from the ECDC are the following:

- ECDC staff members
- ECDC's contractors
- Public health experts from participating EU and EEA countries
- Public health experts from participating EU Candidate countries
- Public health experts from other public health collaborating countries
- Experts from other stakeholders (EFSA, EC, WHO)
- Member States and EEA experts nominated by the Coordinating Competent Bodies (for public health experts)
- Experts from non-EEA countries nominated by the national public health authorities
Pseudo-anonymised patient data may be transferred to recipients in third countries or international organisations, for example, Centres for Disease Control and academic institutions for the purpose of improving control of CCRE through surveillance and related research.

The HMA-EMA Joint Big Data Taskforce Phase II report (Heads of Medicines Agency & European Medicines Agency, 2020) makes several recommendations for the European medicines regulatory network¹⁷⁸ to transform its approach to data use. The most ambitious of these recommendations is the establishment of an EU platform to access and analyse healthcare data from across the European Union (Data Analysis and Real World Interrogation Network, or DARWIN). This platform would create a European network of databases of verified quality and content with the highest levels of data security. It would be used to inform regulatory decision-making with robust evidence from healthcare practice.

Box 42. Darwin initiative

DARWIN is a big data initiative at an EU scope, which will establish a network of data, expertise, and services to support better decision-making by EMA and NCA scientific committees on the benefits and risks of products via rapid access and analysis and increased reliability, validity and representativeness of EU health data in order to (Domergue et. Al. 2020):

- complement clinical trials and support the development, authorisation and supervision of medicines: supports patient access and, safe and effective use;
- support the development of innovated medicines, deliver life-saving treatments to patients more quickly and optimise the safe and effective use of medicines through monitoring of a products performance on the market;
- support early access to medicines thereby fulfilling the unmet medical needs of EU citizens,
- support a learning healthcare system for marketed products enabling safe and effective use of medicines; and establish evidentiary value of real-world evidence.

¹⁷⁷ https://www.ecdc.europa.eu/sites/default/files/documents/privacy-statement-CCRE_0.pdf

¹⁷⁸ <https://www.ema.europa.eu/en/glossary/european-medicines-regulatory-network>

Cross-border access to health data for policymakers and regulators has never been more imperative as now, with the current state of the COVID-19 pandemic. With this cross-border and global threat to health, the call for policy-makers to open health data for research has grown stronger and as a response, in April the European Commission reacted by establishing the COVID-19 Data Platform, a data portal that allows researchers to rapidly collect and share data on the coronavirus.¹⁷⁹¹⁸⁰ Countries with strong data coordination structures have an advantage of being able to respond more quickly to the cross-border threats due to the swift exchange of information.¹⁸¹ The COVID-19 crisis is therefore a case scenario that shows the importance of improving better health data sharing across Member States.

When discussing primary purposes, the High-Level Expert Group on Business to Government (B2G) data sharing, an independent expert group set up by the European Commission in November 2018, has identified good practices of successful public-private partnerships in the e-health sector. An example of these is a B2G data sharing between Roche and Romanian Public Institute of Oncology 'Prof. Dr Ion Chiricuta' Cluj-Napoca (IOCN). In Romania the presence of women with advanced breast cancer who are still in good physical shape, yet had exhausted other therapeutic options, stressed the need to use new molecular profiling technologies to identify new personalised treatments. However, these technologies had not yet seen a large-scale adoption in the local clinical practice in Romania because of its high economic costs.

The Roche partnership provided women with advanced breast cancer with a genomic profiling technology (free of charge) to identify personal treatments. The raw genome-sequencing data of each patient was collected and processed by Foundation Medicine (an asset of Roche), which shares the insights from the data with IOCN. The oncologists at IOCN then select the eligible patients and discuss the outcomes within the Romanian breast tumour board.¹⁸² This anonymised and aggregated genome-sequencing data, and the newly identified treatment options, are also introduced in an electronic health records (EHR) platform owned by ICON. A statistical analysis is performed on the existing data in order to extract relevant insights. Finally, the genome-sequencing data was anonymised and aggregated before being published by the investigators, and can be used for future clinical decision support as well as health-care policymaking. In this case the purpose of this B2G partnerships was multilateral; it used health data for primary purposes (to provide healthcare services), and secondary purposes (for research and to support health-care policy making).

A recent collaboration that reflects the importance of data exchange among businesses and health authorities is the **Accumulus Synergy project**¹⁸³, a non-profit which aims to develop a data sharing platform to transform the way the biopharmaceutical industry cooperates with health authorities. This project comprises of 10 of the leading pharmaceutical companies: Amgen, Astellas, Bristol Myers Squibb, GSK, Janssen, Lilly, Pfizer, Roche, Sanofi and Takeda. The Accumulus Synergy project plans to improve efficiencies in the regulatory process by leveraging advanced technology, including AI, and data exchange to improve patient safety, assist with the reduction of innovation costs, and accelerate the development of safe and effective medicines. This non-profit will partner with companies, global health authorities, and

¹⁷⁹ https://ec.europa.eu/commission/presscorner/detail/en/IP_20_680

¹⁸⁰ For example, the European Network of Cancer Registries collects on cancer for policy making. [ENCR | European Network of Cancer Registries](#)

¹⁸¹ <https://www.technology.org/2020/09/16/coronavirus-accelerates-drive-to-share-health-data-across-borders/>

¹⁸² <https://ec.europa.eu/digital-single-market/en/news/good-practice-b2g-data-sharing-romanian-breast-cancer-molecular-profiling-tumour-board>

¹⁸³ <https://www.accumulus.org/#about>

other stakeholders to build and sustain a cloud-based platform that meets regulatory, cybersecurity, and privacy requirements spanning clinical, safety, chemistry and manufacturing, and regulatory exchanges and submissions¹⁸⁴.

Non-EU/EEA stakeholder access to health data in the EU

Benefits of international transfers and access of health data are essential for innovations in public health and biomedicine. The GDPR (Article 3) protects the rights of individuals in the EU in relation to their personal data. It applies to organizations that handle such data whether they are EU-based organizations or not. Specifically, chapter 5 of the GDPR also provides rules and mechanisms to transfers of personal data to third countries or international organisation.

Box 43. Chapter 5 Transfers of personal data to third countries or international organisations

The three basic mechanisms for a legal international transfer of data, detailed in Chapter 5 of the GDPR, include:

- Article 45 Transfers on the basis of an 'adequacy decision' by the EC;
- Article 46 & 47 Transfers subject to 'appropriate safeguards' by the controller/processor on condition that enforceable data subject rights and effective legal remedies for data subjects are available; and
- Article 49 Derogations for specific situations.

The Data Governance Act also provides the possibility to lay down limitations to transfers of non-personal highly sensitive data for public interest grounds.

When considering exchanges of health data between the EU and USA researchers and patients on both sides of the Atlantic require rules that protect the fundamental rights of individuals although also allowing research on treatments and therapeutics to move forward as swiftly as possible (Bradford et. Al. 2020). In fact, the USA, as well as the majority of countries around the world, is cited as not adequately safe for data exchange by adequacy decision of the European Commission¹⁸⁵.

In Member States, international organisations or researchers can have access to health data, such as Finland and Germany. However, international organisations may be subject to higher fees due to additional bureaucratic procedures that have to be followed. An example of this is Finland, which charges EUR 1,000 from EU/EEA countries for a data permit application as compared to EUR 3,000 for an organisation from a non-EU/EEA country. In fact, barriers for international organisations, looking to access certain Member States health data, may include do not only include the possibility of higher service fees but difficult and disjointed regulatory landscapes, higher service fees, and language barriers. For example, in Germany non-EU institutions of health research are able to apply to have access to the data however, the application can only currently be made in German.

¹⁸⁴ Ibid.

¹⁸⁵ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

4.2 Regulatory landscape

4.2.1 Health data exchange for healthcare provision (primary purposes)

The basis for eHealth services are found both at the EU level and the national level. At the EU level there is legislation on eHealth, such as the Cross-Border Healthcare Directive (2011/24/EU), and there are EU organisations implementing electronic health records such as ERNs. At the national and regional level there are laws and institutions implementing electronic records at a national and regional level. The 2011/24/EU Directive allows for the functioning of the eHealth Network, a voluntary network for the collaboration on digital health in the EU. To promote health data exchange across borders, the EC has set up MyHealth@EU.

Electronic health records and patient access

A final report¹⁸⁶ on the overview of the national laws on electronic health records in the EU Member States and Norway and their interaction with the provision of cross-border eHealth services published in 2016 uncovered major disparities between countries on the deployment of electronic health records as part of an interoperable infrastructure that allows different healthcare providers to access and update health data in order to ensure the continuity of care of the patient.

Box 44. National eHealth portal in Denmark

The national eHealth portal – Sundhed.dk (<https://www.sundhed.dk>) allows Danish patients to access their medication profiles, view scheduled consultations with healthcare providers, and re-order certain medication themselves¹⁸⁷. In 2018, the Danish authorities were working on a pilot project to add further features to the eHealth portal so as to make it easier for patients who consult the doctor frequently (e.g. for chronic disease patients) to schedule their appointments.

In addition, the “Medicinkortet” mobile application allows patients to request an extension for their existing digital prescriptions. All medical prescriptions issued in Denmark are digital.

Source: European Court of Auditors (2019)

By the stage of completion of the report mentioned above, 17 EU member states had specifically regulated the content of EHRs. This legislation, however, was often specifically applicable to shared EHR systems. The Czech Republic Germany, Ireland, and Slovenia were only at the stage of policy initiatives to develop shared EHR systems. Croatia, Greece, Latvia, Norway, and Romania were testing shared EHR systems at the pilot phase. Austria, Belgium, Cyprus, France, Italy, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Slovakia were in the process of deploying EHR systems. Finally, EHR systems were fully implemented in Bulgaria, Denmark, Hungary, Estonia, Finland, Malta, Netherlands, Sweden and UK.¹⁸⁸ Two broad legislative approaches were distinguishable. First, while some countries have set detailed requirements as to the content of EHRs¹⁸⁹, others do not specify what this content should be. Second, in some countries with a decentralised system, the legislation defined a common set of health data categories which applied to all regions. A number of countries do not define in detail the content

¹⁸⁶ https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf

¹⁸⁷ Not part of the eHealth Network but deploys eHealth services.

¹⁸⁸ At the time of the aforementioned report, the UK was still a Member State.

¹⁸⁹ Existence of detailed requirements were identified for: Austria, Belgium, Estonia, Greece Spain, Finland, Croatia, Italy, Luxembourg, Latvia, Norway, Portugal Slovakia, Sweden, UK.

of EHRs, either because they do not have shared EHR systems created or planned, or because they do not distinguish between electronic and paper-based health records, shared or not. Several countries did not restrict the EHRs to contain only health related data.

Table 42. Examples of different legislative requirements for the EHRs in Member States

Country	Description
Croatia	EHRs also include information on insured person's work and profession related data, but also specific habits (smoking, alcohol drinking and addiction to drugs).
Denmark	The name of patients' relatives must be specified.
Estonia	EHRs must include the patient's employer and profession, description of work conditions, educational institution, the family situation, health habits, psychosocial background and development, mental background and development.
France	EHRs include a section on prevention which will cover medico-social information.
Greece	Medical records must also contain the father's name and the occupation of the patient.
Hungary	The profession of the patient must be included.
Italy	EHRs contain, in addition to health data, 'socio-health' data (no clear definition of what this covers is provided).
Luxembourg	The law allows the patient to complete a section of the EHR where he/she can provide additional information or declarations.
Slovenia	The marital status, the education and the profession of a patient must be included in EHRs.
Spain	The occupation of a patient must be indicated.
Sweden	Allows information to be included about criminal offences of a patient, only if there is an absolute necessity to do so.
Romania	Discussing the possibility of adding in the EHRs information on religion, occupation, lifestyle/behaviour, family history. There is however no legal initiative for the moment and the current EHRs are restricted to health data

Source: Milieu (2014)

With the entry into application of the General Data Protection Regulation, the processing of patient information must adhere to its provisions. However, the diversified way of keeping and protecting EHRs leads to individual application of GDPR rules to each register or database. A report by the eHealth Network (2019)¹⁹⁰ revealed that many countries encountered problems related to the processing of patient data and its compliance with the GDPR, covering a broad range of issues such as:

- health service provider did not inform data subjects about phone call recording;
- poor processing of paper medical records: the proper physical security was not secured;
- a psychiatric hospital revealed information about a patient's private life to journalists;
- patients were blackmailed: data stolen from a plastic surgery clinic;

¹⁹⁰ http://eaction.eu/wp-content/uploads/2020/05/3.1_D7.2-Best-practices-report-on-data-protection-at-national-level-eHAction_16th-eHN ANNEX.pdf

- complaint against a health professional due to non-eligible access to healthcare documentation;
- a large hospital published patient data in the press;
- a stolen computer included patient data;
- a university hospital's invoices included patient data.

The study commissioned by the EC (2021) revealed that within the context of sharing data, some countries provide the opportunity to transmit health care provider-controlled data held in an EHR to a record controlled by a patient, such as a PHR or other system by which a patient can directly access data held by HCPs. Access to EHR data via an online portal is by far the most common mode of access in Member States; another four Member States report offering mobile access while two Member States still use paper printouts (note that multiple answers could be valid for a single country)¹⁹¹.

Table 43. Legislation or rules that facilitate data from the EHRs to be used/controlled by patients

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

Source: EC (2021)

Existing EU laws

The use and sharing of health data are subject to core EU Single market principles of free movement of people, goods and services, as well as EU citizen's fundamental rights to privacy and to the protection of personal data. eHealth, and the exchange of patient data by electronic means can positively contribute to reinforcing patient's rights in cross-border healthcare. The processing of health data, however, gives rise to a number of challenges. Importantly, while it becomes clear that many countries have implemented changes in their national legislation as a result of the GDPR in the area of health, some countries are still facing challenges to adapt the relevant sectoral legislation (European Commission, 2020).

The **GDPR harmonises the rules governing the processing of sensitive data**, such as personal health data, but there are still options for Member States to lay down legal ground for derogation (as provided by Article 9(4) of the GDPR) for processing health data in Member States law. Article 9(4) explicitly provides that with regard to processing of genetic, biometric or health data, Member States may maintain already existing legislation or introduce further restrictions or conditions. The resulting differences may affect the cross-border exchange of health data for different purposes (primary and secondary uses), also because the rules under the GDPR

¹⁹¹ From the forthcoming European Commission report "Interoperability of Electronic Health Records in the EU SMART 2019/0056"

applicable to processing of health-related data will be applied in the health system specific legal context of each Member States (EC, 2020).

In concrete, this means that one Member States may lean more towards the use of consent, and another to incline more towards the legal obligation to record all aspects of interaction of a patient with the healthcare system.

The national organisation of the health system may also mean that the legal base chosen varies between different categories of care providers, with publicly funded healthcare organisations applying different bases to private healthcare providers, indeed this variation was noted by the correspondent providing information on the application of the GDPR in Spain.

A number of Member States may also have legislation that provides conditions or limitations to the processing of health data or genetic data (as permitted under Article 9(4) GDPR).

Box 45. Examples of variation across countries caused by the application of stricter rules at national level: France and the Netherlands

French law prohibits the automatic processing of genetic data unless express authorisation is given by the French competent authority (French Data Protection Act Loi n° 78-17 19783);

Dutch implementing Act of the GDPR prohibits the processing of genetic data unless that processing ‘takes place with respect to the data subject from whom the data concerned have been obtained’.

However, both French and Dutch law contain significant exceptions permitting such data to be used for medical purposes. In France, this includes processing by doctors or biologists which is necessary for preventive medicine, diagnosis and care (Loi n° 78-17 1978). In the Netherlands, the processing of genetic data may also take place for others than the data subject whose data it concerns if a significant medical interest prevails (Article 28, section 2 of the implementing Act (UAVG)). Medical confidentiality will then prescribe that notifying those others will be based on consent of the data subject concerned, though in exceptional cases the genetic counsellor can also fall back on the ‘conflict of interests’ doctrine in Dutch medical law, in essence stating confidentiality can be waived if that is the only likely way to avoid a life-threatening situation of another party.

Below we highlight how different countries apply different legal bases for the processing of health data.

Table 44. Legal bases for primary use of health data (normal healthcare provision)

Legal basis for processing data for normal healthcare provisions	Applies in the following countries
6(1)(a) Consent and 9(2)(a) Consent	BE, BG, CY, DK, DE, FR, HR, MT, AT, PT, SI, FI
6(1)(c) Legal obligation + 9(2)(i) public interest 9 in the area of public health	DK, GR, ES, HR, LV, MT, PT, RO, SI
6(1)(c) legal obligation + 9(2)(h) provision of health or social care	BE, BG, CZ, DK, GR, ES, FR, HR, LV, LT, LU, HU, NL, AT, PL, PT, RO, SI, SK, FI, SE
6(1)(e) public interest + 9(2)(h) provision of 13 health or social care	BG, DK, EE, IE, GR, LV, LT, LU, MT, RO, FI, SE
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	BE, BG, DK, IE, GR, LV, MT, RO
6(1)(f) legitimate interest + 9(2)(h) provision of 2 health or social care	IE, AT

Legal basis for processing data for normal healthcare provisions	Applies in the following countries
Other combination	DE, ES, IT, LV, HU, AT

Source: EC (2021)

This variation shows that there is a full range of potential legal base combinations across Article 6(1) and 9(2) GDPR used by the Member States, which naturally leads to questions of how cross-border data sharing for planned or unplanned care is handled. It was reported that the application of the provisions of the GDPR can cause issues when cross-border transfer of patient data is necessary. More than half of the Member States commented that the range of potential legal bases in GDPR and the different application of those bases between the Member States could hamper the flow of patient data for care or research purposes between Member States, and about half of the Member States believe it could hamper data flow within their Member States to.

The report on the assessment of the EU Member States' rules on health data in light of GDPR (2021) revealed that all Member States have some form of national level legislation which provides a further framework for the collection and processing of data for healthcare provision purposes, which must be read in conjunction with changes that were made to data protection law made to implement the GDPR. Importantly, this implies that the application of the GDPR in this area must be understood within the context of other laws relating to health data and the provision of healthcare that remain applicable. Almost all the relevant EU countries have established sectoral law preceding the GDPR and much of it is also based within the constitutions of the countries and in common law in the countries where common law applies, with only the correspondents for Denmark and Germany reporting very recent changes to the law that regulates health data processing.

Countries that adopted measures pursuant to Article 9(4) GDPR did so in within three categories of law: (1) laws which address the use of highly sensitive information in the context of the provision of insurance, employment or any other contractual relationship; (2) laws which specifically address the use genetic information in the context of assisted reproduction; (3) and laws which simply require the use of special safeguards or obtaining special permission from the data protection authority when any form of highly sensitive data are used (EC, 2021).

One of the key elements of the **Directive 2011/24/EU** is to set conditions for patients' rights in cross-border healthcare and cooperation between EU countries to provide health information. Specifically, Article 14 of Directive 2011/24/EU foresees the cooperation and exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States. The objective of this eHealth Network (eHN) is to "work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare." (Art. 14, 2a)

Challenges and regulatory gaps for the exchange of health data for healthcare provision

A study conducted for the EC on the Mapping of Patient's Rights in the European Union (2016)¹⁹² concluded that while in many Member States no specific provisions exist for cross-border patients, the existing laws regarding informed consent, data protection or access to the medical

¹⁹² https://ec.europa.eu/health/sites/health/files/cross_border_care/docs/2018_mapping_patientsrights_frep_en.pdf

record equally apply to all health care provided on their territory. One of the specific issues related to the application of patients' rights in the context of cross-border patients highlighted in the study cover informed consent and access to medical record possibly impeded by language problems, choice of provider and information for cross-border patients, procedural rights and continuity of care. The provision of eHealth services in a cross-border situation may require some special attention in some countries.

The report by the eHealth Network¹⁹³ revealed that the **biggest challenge is to ensure data security and effective compliance**. In particular, "*supervisory authorit(ies) consider (the) possibility to look and read patient's data in health databases problematic because it is one of the major concerns and problems that also receives DPA's attention due to data subject's complaints (if patients find out or consider their data has been looked in the databases unlawfully/without purpose/just out of curiosity). To do this, the controller needs to improve the traceability of data processing - for example, to ensure the traceability of his / her processing through the display of logs, to create control mechanisms that are based on loges and automated, etc. It is certainly helpful to share different new technical solutions here. The availability of resources is different for different service providers. This is the question of whether and to what extent the public sector itself can take the lead role to help. The restriction of different rights, where certain roles see only the kind of information that they need, helps to avoid excessive or unintended data processing. At the same time, however, it is highly dependent on the resources of the service provider and who is currently using the information system. The ability and knowledge of different providers is definitely different. From the ministry's point of view, it is important to have guidelines and certification processes that harmonize different ways and methods.*" (p. 45).

The eHealth Digital Service Infrastructure Legal Report (2019)¹⁹⁴ outlined that the current legal bases, enriched by national laws, are sufficient for the first cross-border data exchanges between MS. However, it was highlighted that legal interpretations by the European Commission included in its Recommendation on the Electronic Health Record exchange format may require additional analysis, especially as it contains a legal interpretation on eIDAS Regulation, GDPR and NIS Directive in the context of a European Electronic Health Record exchange format which will to some extent take advantage of the eHealth Digital Service Infrastructure (eHDSI) at least in terms of its existing CBeHIS (Cross-Border eHealth Information Services), namely Patient Summary and ePrescription. Some open legal points will be further elaborated upon by the eHealth Network in collaboration with the eHealth Member State Expert Legal Working Group.

Another important gap remain clear issues related to the consent management of data, as a patient's consent must be also exchanged among different Member States when a patient is being assisted by a doctor in other country (Larrucea, 2020). The GDPR prescribes that a "statement or clear affirmative action" is a prerequisite for 'regular' consent (Article 4(11)). As the 'regular' consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the explicit consent of a data subject in line with the GDPR. The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent.

¹⁹³ http://eaction.eu/wp-content/uploads/2020/05/3.1_D7.2-Best-practices-report-on-data-protection-at-national-level-eHAction_16th-eHN_ANNEX.pdf

¹⁹⁴ https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co222_en.pdf

This issue has been addressed in the EDPB guidance document¹⁹⁵. As suggested in the guidance, the GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages.

However, the GDPR puts additional requirements for informed consent in place, predominantly in Article 7(2) and Recital 32. This leads to a higher standard for the clarity and accessibility of the information. Obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity. The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.

Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49, and in Article 22 on automated individual decision-making, including profiling.

According to the EDPB guidance, an obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement, but in the digital or online context, a data subject may also be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, also the use of oral statements can also be sufficiently express to obtain valid explicit consent, including in a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject. Lastly, also two stage verification (e.g. request to provide consent via email and subsequent email reply containing the statement 'I agree') of consent can be a way to make sure explicit consent is valid.

Whilst setting up data repositories and ensuring interoperability is important, it is equally important to ensure data protection and cybersecurity. As recent ransomware attacks have shown, these could block the activity of healthcare systems for long periods, sometimes with important consequences for patients. To estimate one of the potential costs of cybersecurity breaches, the value of black-market prices (or the value of an individual's health record on the dark web) and extortion, was calculated, shown in Annex 8.5.2. Furthermore, as for previous estimations, all table calculations are detailed in Annex 8.5.1. Black market prices are important to consider because they represent a potential cost of medical and other identify thefts. Often, stolen data will be offered to the compromised organization to extort ransom for fences of stolen data before going public on the black market (Dissent, 2016). According to the OECD (OECD, 2013), analyzing black market prices may even be a more accurate measure of the value of data sets than other suggested measures because illegal data may represent a rival good, i. e., a good in which the value decreases as more customers gain access to it. In this case, the U.S. was considered as the baseline, with estimated market prices for selling and buying health care data as well as response to extortion range between 0.05 USD and 50 USD per record (Czeschik, 2017). These values represent the price of an individual's health record on the dark web. The reason why this range is so large is that many times hackers will offer a "bulk discount" when

¹⁹⁵ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

attempting extortion for high volumes of health data sets. The values of extortion in this report were estimated using this range and taking into consideration PPP. Further research is required for other digital integration costs such as the costs associated with collecting, cleaning raw health data files into consolidated EHRs, maintaining, analysing and protecting health data files.

4.2.2 Health data access for research, innovation, policy making and regulatory decision (secondary purposes)

Secondary uses of data for wider public health purposes include the 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 medical products and medical devices. **Other secondary uses also include carrying out research.** The data used for these purposes includes those that were collected initially in the context of providing care, but then re-used for secondary uses by public entities such as national health systems statutory payers, public health bodies and regulators such as medicines agencies (EC, 2021).

Article 9(1) of the GDPR notes that in general processing of data concerning health or genetic data shall be prohibited, but provides in 9(2) that this prohibition will not apply if the data subject has given explicit consent or, in the case of health related data, that additional national or EU level legislation has been adopted that addresses the processing of health data for the purposes of providing healthcare (9(2)(h)) or for public health reasons (9(2)(i)) **or for research purposes (9(2)(j))**

Table 45. Legal bases for processing data for secondary purposes

Legal bases for healthcare management	Applies in the following countries
6(1)(c) Legal obligation + 9(2)(i) public interest in the area of public health	CZ, DK, DE, IE, GR, ES, HR, LV, LT, LU, HU, NL, PL, PT, SI, SK, FI
6(1)(c) legal obligation + 9(2)(h) healthcare	DK, IE, GR, ES, FR, HR, LV, LT, SI, SE
6(1)(e) public interest + 9(2)(h) healthcare	BG, DK, EE, IE, GR, ES, FR, HR, LV, LT, MT, AT, SE
6(1)(e) public interest + 9(2)(i) public interest in the field of public health	BG, CZ, DK, EE, IE, ES, LV, LU, MT, NL, AT, FI
6(1)(f) legitimate interest + 9(2)(h) healthcare	IE
Other combination*	DK, DE, GR, ES, IT, MT
No specific legislation	BE, CY, RO

Source: EC (2021)

Table 46. Sectoral legislation or authoritative guidance by Member States in the context of health research

MS has adopted sectoral legislation or authoritative guidance specifying safeguards to be applied in line with Art. 89 in the context of health research	Total	MS
No	10	CZ, FR, CY, LT, HU, NL, PL, PT, SK
Yes	19	BE, BG, DK, DE, EE, IE, GR, ES, HR, IT, LV, LU, MT, AT, RO, SI, FI, SE
If yes, the following issues are addressed specifically in the legislation		
Scientific research by public sector organisations	12	BG, DK, DE, EE, GR, ES, HR, LU, MT, AT, FI, SE
Scientific research by private sector organisations	10	DK, DE, EE, GR, ES, LU, MT, AT, FI, SE
Research for development of national statistics	12	BG, DK, DE, EE, GR, ES, HR, LU, MT, AT, RO, FI
Research for authorities' planning	9	BG, DE, EE, ES, HR, LU, MT, RO, FI
Other, please explain	7	BE, IE, ES, IT, LV, RO

Source: EC (2021)

As shown in the tables above, many countries have more than one legal basis for processing data originally collected for the purpose of providing care to allow it to be used for planning, management, administration and improvement of the health and care systems. The legal bases used within one Member States usually depends upon the type of processing: for management and planning of the health care system, reimbursement or improvement. The legal bases used also depends upon the actors involved and characteristics of the health care system. There exists a number of differences between taxation based and insurance-based systems and whether there is a large private health insurance sector. In the latter case legitimate interest (6(1)(f) GDPR) will often be the residual legal basis. In the absence of any specific legislation, implementing 9(2)(h) or 9(2)(i) GDPR, only 9(2)(a)GDPR, explicit consent, would be the basis to open-up data to meet the needs of planning and reimbursement. Furthermore, in the case of reimbursement the validity of consent would be questionable as valid consent means that the data subject should also be able to refuse to give consent without negative consequences (European Data Protection Board's (EDPB) Guidelines 05/2020 on consent under Regulation 2016/679). Health system management often includes collaboration between healthcare provider and public health bodies, which is governed by specific legislation, which differs significantly across countries. Sectoral legislation can oblige a health care provider to give public health authorities access to patient data for the management of the health care system as shown in the following box:

Box 46. Examples of specific legislation that obliges healthcare providers to provide patient data to public health authorities*

In **Bulgaria**, legislation can be related to the use of data for the needs of public healthcare (under the National Health Act, art. 28/4). The information must be anonymized or de-identified. This is similar to the situation in Ireland. In contrast, in Lithuania, the State Accreditation Service for Health Care Activities has the right to receive all information, including personal data from healthcare institutions when this is required to assess compliance with the requirements of the legislation (under the Law on Health Care Institutions in order to ensure the adequacy of personal healthcare services and patient safety).

In **Italy**, the Regions, the Province, the Ministry of Health and the Ministry of Labour have the possibility to access health data for governance purposes (as described in art. 12 paragraph 2 letter c) of Legislative Decree no. 179/2012 and by Articles 18 and 19 of Decree no. 178/2015). These data can be processed "as long as they are deprived of direct identification data of the patient and in accordance with the principles of indispensability, relevance and not excessive in relation to these purposes".

In **Greece**, Law 4624/2019, Article 22 (paragraph 1b and 2b) implements the GDPR into Greek legislation and states that by way of derogation from Article 9 (1) of the GDPR, the processing of special categories of personal data, in the sense of Article 9 (1) of the GDPR by public authorities is allowed, if it is necessary for, among others: for reasons of preventive medicine, for the assessment of the employee's ability to work, for medical diagnosis, for providing health or social care or for the management of systems and health or social care services or potential contract with a healthcare professional or other person bound by professional secrecy or is under his supervision.

In **Sweden**, according to the Act (1998: 543) on health data registers, all health care providers are obliged to provide patient data to a health data register kept by the National board on Health and welfare, the Medical Products Agency and the Public Health Agency. But the purpose must be 1. Production of statistics, 2. Follow-up, evaluation and quality assurance of health care, or 3. Research and epidemiological investigations.

In the **Netherlands**, data must be pseudonymised.

A number of countries have legislation in place to allow secondary use of data for public health purposes.

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

Source: Source: EC (2021)

Health data can further be processed by insurers, indicating that there is a health data flow between healthcare providers and insurers that is regulated by national legislation, which may oblige health care providers to release patient data to an insurer. A number of countries oblige insurance companies to obtain specific consent about data releases and thus, release to an insurer can only be made if such consent is shown. If consent cannot be proven, then the healthcare provider must refuse to provide patient data to an insurer. A distinction must be made however between additional insurance taken out by a patient as a private contact and the insurance bodies which service the national health systems of Member States.

Box 47. Example of legislation on providing health data to insurers

In **Sweden**, health data may only be shared with an insurer after the explicit consent of the patient. Furthermore, the Act (2006:351) on Genetic integrity prevents insurer from asking patients for granting access to genetic information. If the data may be withheld from the patient (see above under 2 b), it may also be withheld from insurers, even if the patient consents to the transfer of the data from the care provider to the insurer.

Source: EC (2021)

Challenges and regulatory barriers for the access of health data for research, innovation, policy making and regulatory decision (secondary purposes)

As it has been mentioned in the EHDS combined evaluation roadmap/ inception impact assessment,¹⁹⁶ the current situation of fragmentation, differences in and barriers to access health data in the cross-border context, including by patients, researchers and policy-makers, as well as limited interoperability, shows that action by Member States alone is not sufficient and that it requires a common framework at EU level, as suggested by the DGA. Member States deploy different legal bases which typically depend on the type of processing, e.g. for management and planning of the health care system, reimbursement or improvement. At EU level, sector-specific legislation on data access is under preparation to address the health sector. Setting up a health data space will be part of building a European Health Union, a process launched by the Commission on 11 November 2020 with a first set of proposals to reinforce preparedness and response during health crises. It is also a follow-up of the European data strategy adopted in February 2020, in which the Commission had stressed the importance of creating European data spaces, including on health.¹⁹⁷ From a regulatory perspective, the proposed Data Governance Act brings some new elements for governance of data spaces, but specificities of health data require further legislative action.

As suggested by the eHealth Network¹⁹⁸, while policies and regulations might be regarded as very permissive in some countries, the national laws in other countries are considered as very stringent, thus impeding the information sharing between healthcare professionals as well as for secondary purposes such as scientific research. For this purpose, some countries are reconsidering their initial adaptation of the GDPR. Finding such a balance, even at national level, is not easy nor set in stone indefinitely, but if such a balance is not met and secured in clear regulations, then this can also impose a major barrier of citizen acceptance of certain digital health innovations. Placing this into an EU context the issue is even more problematic, as divergence in legal rules governing the use of health data especially for secondary purposes is seen at both within and between countries. Member States and the EU are faced with several challenges in this respect.

According to the Report by the eHealth Network¹⁹⁹, the key impact of the GDPR on national authorities and organisations collecting patient data, healthcare documentation or electronic health records is additional workload carrying forward necessary secondary legislation, many legislative acts at a national level still being revised and amended, increased importance to

¹⁹⁶ See Proposal for Regulation [tbc] on the European Health Data Space, digital health services and products and the use of new technologies, including artificial intelligence (AI) in health [https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares\(2020\)7907993](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=PI_COM:Ares(2020)7907993)

¹⁹⁷ <https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-european-health-data-space>

¹⁹⁸ http://ehaction.eu/wp-content/uploads/2020/05/3.1_D7.2-Best-practices-report-on-data-protection-at-national-level-eHAction_16th-eHN ANNEX.pdf

¹⁹⁹ Ibid.

health data often leads to withholding without reason (even though the state authorities have the right to receive it), increased complexity of the administrative processes, pseudonymisation problems, or dual practice. The collection, retention, and cross-border exchange of health data however raises questions about data protection and the provision of consent (Arak, 2017).

One important inhibitor continues to be the varying levels of eHealth services in the Member States and the resulting gaps of interoperability between different electronic health records, which, if not addressed, will result in continued fragmentation and a lower quality of cross-border healthcare provisions, as it will not be possible to process information in a consistent manner between different health information systems, regardless of their technology, application or platform in a way that it can be meaningfully interpreted by the recipient. If the possibility of having unified and digitalised patient data is limited, the secondary use would be limited too. Moreover, gaps remain as concerns secondary uses of data in particular in cross-border settings as well as the standardisation of processes for access to health data across Member States, the lack of infrastructures, and inconsistencies in data quality of collected data. Clearly, there is a push for data interoperability articulated by policy makers but there is no mandatory obligation to ensure operability at national level. There is no binding EU-level action for infrastructure and IT when setting up interoperability structures at national level (further expanded on in chapter 5).

5. Evaluation of Article 14 of Directive 2011/24/EU

5.1 Description of the initiative and its objectives

The adoption of the Directive 2011/24/EU was an important step in respecting patients' rights in cross-border healthcare, with consequences both for the health of patients and for the health systems in the Member States. The **overall objective** of the Directive 2011/24/EU is to **facilitate the access to safe and high-quality cross-border healthcare and promote cooperation between Member States.**

The lack of cooperation among healthcare providers, purchasers and regulators of different Member States at national, regional or local level may hamper safe, high-quality and efficient cross-border healthcare. This could be of particular importance in border regions, where cross-border provision of services may be the most efficient way of organising health services for the local population, but where achieving such cross-border provision on a sustained basis requires cooperation between the health systems of different Member States. Such cooperation may concern joint planning, mutual recognition or adaptation of procedures or standards, interoperability of respective national information and communication technology (hereinafter 'ICT') systems, practical mechanisms to ensure continuity of care or practical facilitating of cross-border provision of healthcare by health professionals on a temporary or occasional basis.

In the field of ICT, Article 14 of the Directive 2011/24/EU states that *the Union shall support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States*. This commitment resulted in the setting-up of the **eHealth Network**. The network was assigned with the following **specific objectives**:

Box 48. Specific objectives of the eHealth Network

- Support economic and social benefits of European eHealth systems and services and interoperable applications
- Support interoperability of ICT systems, including at national level and support access of patients to their health data, especially through guidelines
- Achieve a high level of trust and security
- Enhance continuity of care
- Ensure access to safe and high-quality healthcare
- Facilitate European cooperation on using ICT to provide more efficient healthcare
- Facilitate the exchange of patients health data across borders to enable continuity of care and patient safety across borders
- Support the consistent use of ICTs in healthcare (eHealth) in the EU and to achieve the interoperability of Member States' ICTs
- Support the innovative use of health data for secondary purposes including across borders

Source: Author's elaboration

In operative terms, the initiative tried to specify and implement semantic, legal and technical requirements for the **interoperability of eHealth**, as well as for the standardisation of **patient summaries, electronic prescriptions** and other domains. To do so, the network had to develop and implement a **common secure identification and authentication system of patients** and healthcare providers. Furthermore, the network was requested to define and deploy **effective methods and requirements to enhance the use of data for secondary purposes**. The mandate of the eHealth Network was defined rather broadly in the context of the Directive 2011/24/EU. This allowed a very strong collaboration in the context of the COVID-19 crisis, which has increased significantly the cooperation within eHealth Network, leading to

significant standardisation at Member States level and cross-border interoperability (eg for contact tracing and warning apps and EU Digital COVID Certificates).

Box 49. Operational objectives of the eHealth Network

- Support interoperability of ICT systems, including at national level and support access of patients to their health data, especially through guidelines
- Specify and implement semantic, legal and technical requirements for the interoperability of eHealth
- Specify and implement semantic, legal and technical requirements for the standardisation of patient summaries, electronic prescriptions and other domains, , (as part of the interoperability of electronic health records)
- Develop and implement a common secure identification and authentication system of patients and healthcare providers
- Define and deploy effective methods and requirements to enhance the use of data for secondary purposes
- Develop other EU-wide interoperable infrastructures and applications

Source: Author's elaboration

These objectives were intended to overcome existing **needs** and to ensure that if patients receive healthcare services in another Member States, this happens within a clear and secure framework and that **continuity of care** is ensured wherever the patient is treated and after they return to the Member States of affiliation. To allow this continuity of care, the need arose to overcome the existing **lack of technical, semantic, and organisational interoperability between national eHealth systems** and to ensure **citizens' secure access to and sharing of health data across borders**, while **enabling citizens to take an active role in the management of their own health data**, including in the area of e-health, m-health and telemedicine as specified in the EU e-Government Action Plan 2016-2020 (see section 5.3.5). These European developments also had impact at national level in terms of interoperability, standardisation etc.

Having interoperable platforms can also enable the collection and **re-usage of health data to advance research, disease prevention and personalised health and care**. Furthermore, as also highlighted by the recent COVID-19 pandemic, building better interoperable health databases is also needed to **improve policy action and reaction**.

Box 50. Intervention logic framework: Needs

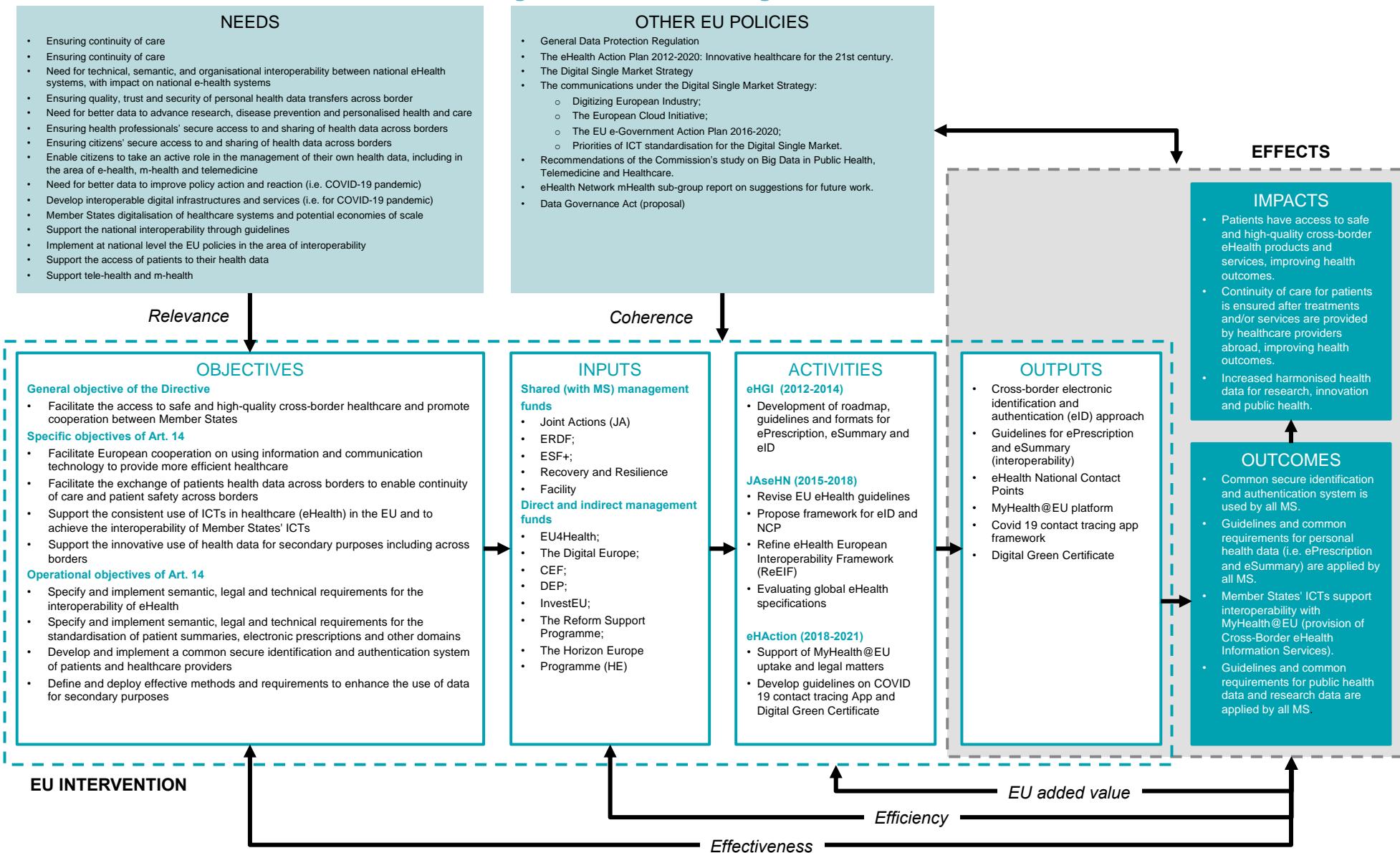
- Ensuring continuity of care
- Need for technical, semantic, and organisational interoperability between national eHealth systems, with impact on national e-health systems
- Ensuring quality, trust and security of personal health data transfers across border
- Need for better data to advance research, disease prevention and personalised health and care
- Ensuring health professionals' secure access to and sharing of health data across borders
- Ensuring citizens' secure access to and sharing of health data across borders
- Enable citizens to take an active role in the management of their own health data, including in the area of e-health, m-health and telemedicine
- Need for better data to improve policy action and reaction (i.e. COVID-19 pandemic)
- Develop interoperable digital infrastructures and services (i.e. for COVID-19 pandemic)
- Member States digitalisation of healthcare systems and potential economies of scale
- Support the national interoperability through guidelines
- Implement at national level the EU policies in the area of interoperability
- Support the access of patients to their health data
- Support tele-health and m-health

Source: Author's elaboration

Following the example set forward by the better regulation guidelines, this evaluation tries to capture the effectiveness, efficiency, relevance, coherence and EU added value of the provisions on eHealth cooperation in the Directive 2011/24/EU (article 14). The initial research question guiding the study are provided in Annex 8.1.

The needs and objectives described in this section have been summarised in the intervention logic provided below. More information on the implementation state (inputs provided, activities carried out, outputs reached, impacts observed and other relevant EU policies affecting the intervention) is provided in the following sections.

Figure 7. Intervention logic framework



Source: Author's elaboration

5.2 Baseline

Since 1998, the construction of a new legal framework to enable cross-border care for citizens has been debated in the EU. While existing legal instruments for organizing free movement of professionals and patients have been reviewed and modernized, the ECJ²⁰⁰ has played an important role in further extending entitlements to cross-border care. By means of proposing a new Directive on the application of patients' rights in cross-border health care, the European Commission initiated a new phase in the political debate in July 2008, which will be taken as our baseline period.

At the time, lack of interoperability of digital health services systems was identified as one of the major obstacles for realising the social and economic benefits of eHealth in the Union. Market fragmentation in eHealth was aggravated by the lack of technical and semantic interoperability. Before the implementation of the Directive 2011/24/EU, the health information and communication systems and standards used in Member States were often incompatible and did not facilitate access to vital information for provision of safe and good quality healthcare across different Member States. **Although some digital registries were already available at national or local level, the different systems were not necessarily interoperable at national level at even less in the context of cross-border healthcare.** Sharing of health data for continuity of care nationally, but also after seeking treatment services abroad where often carried out in a manual fashion by requesting hard copies and translations to the respective healthcare providers.

At the EU level, some EU financed projects such as epSOS and STORK started testing the digital cross-border sharing of certain health data (patient summary and ePrescription) and started to develop framework for cross-border electronic identification and authentication (eID). The results of these initiatives constituted a starting point for the development of the eHealth Network activities although they have been revised multiple times since then.

At that time, **no voluntary network was set up to deal with the complex set of framework conditions, organisational structures and implementation procedures required to achieve and maintain national and cross-border interoperability of digital health services.** Since 2008²⁰¹, the EC already identified technical, semantic, and organisational interoperability as essential to build and ensure interoperable digital health services that could ensure continuity of care. These data transfers had to ensure data quality, trust and security of personal data. Furthermore, quality pan-European data for secondary purposes (research, innovation and public health) were very limited due to national fragmentation. Some exception can be found in few key areas such as rare diseases, where the European Union has supported the field since 2007 with ad-hoc projects under the Seventh Framework Programme²⁰².

A study from 2008²⁰³, highlighted that while patient data were stored electronically in many European GP practices and that computers were available in most GP consultation rooms, **use rates of electronic connections to other health actors were low as were the use rates in the area of electronic transfer of patient data.**

²⁰⁰ Court of Justice of the European Communities ('European Court of Justice') in Decker (C-120/95, 28 April 1998), Kohll (C-158/96, 28 April 1998), Geraets-Smits & Peerbooms (C-157/99, 12 July 2001), Vanbraekel (C368/98, 12 July 2001), IKA (C-326/00, 25 February 2003), Müller-Fauré & van Riet (C-385/99, 13 May 2003), Inizan (C-56/01, 23 October 2003), Leichtle (C-8/02, 18 March 2004) and Watts (C-327/04, 16 May 2005)

²⁰¹ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:190:0037:0043:EN:PDF>

²⁰² https://ec.europa.eu/info/research-and-innovation/research-area/health-research-and-innovation/rare-diseases_en

²⁰³ <https://op.europa.eu/en/publication-detail/-/publication/7d72981d-f924-4977-a032-37361bb8b4b3>

Administrative patient data were stored electronically in 80% of the EU27 GP practices. In some countries, usage rates were below the 50% level (Greece, Romania, Lithuania), going down as far as 26% (Latvia). The highest use rates were found in Denmark (97%), Estonia (98%), Hungary (100%), the Netherlands (97%), Finland (100%) and Sweden (96%). While computers were found in the consultation room of 78% of the European GP practices, they were not always used during consultation with a patient: 66% of the practitioners did so, while in 12% of the practices the computer was not used while a patient was present.

About 21% of European GP practices connected to other primary care actors, i.e. other GPs. Between GP and hospitals and specialist practices there was a noticeable gap. While about one fifth of GP practices connected to hospitals only somewhat more than one tenth (12%) did the same with specialist practices. Connection to pharmacies were considerably less frequent (used by about 7% of the practices). **Medical data were transmitted to care providers or other professionals by 10% of the EU27 GP practices, ePrescription was practiced by 6% of the EU27 GP practices.**

While Article 14 implementation was initially seen especially from the perspective of interoperability across Member States²⁰⁴, it is very important to note that **at the time of the introduction of Article 14 Member States had low use rates of electronic connections and electronic transfer of patient data within their systems.** Since this initial exercise, other benchmarks have been conducted²⁰⁵ showing an increase in the digitalisation of health systems, including interoperability within each Member States and to less extent between Member States. Attributing causality between this digital expansion and the Directive 2011/24/EU is challenging as cross-border care is relatively marginal compared to the overall healthcare provided by the different Member States. Furthermore, such causality is not within the scope of this study.

5.3 Implementation state of play

5.3.1 Input

The activities carried out by the eHealth network have been supported by a wide range of financial instruments such as Joint Actions, the Connecting Europe Facility, European Grants, eHealth Action Plan, etc. The **Joint Actions** (JAs) supporting the eHealth Network have been financed through the **EU Health Programme**, a funding instrument to support cooperation among EU countries and underpin and develop EU health activities. JAs are usually also co-financed by Member States authorities as well as different DG. Overall, we have observed an increase in budget and input provided overtime to eHealth Network activities. For example, the financing of the first JA was of €2.503.791 (see figure below), increased to €4.000.000 in the following JA (JAseHn) and to €4.499.963,46 in the last JA (eHAction). While in the first JA DG SANTE contributed to 50% of the JA financing and additional financing came from DG INFSO

²⁰⁴ As well as patients and healthcare providers' safe access to the transferred health data.

²⁰⁵ Codagnone, C., and F. Lupiáñez-Villanueva.(2011) "A Composite Index for the Benchmarking of eHealth Deployment in European Acute Hospitals Distilling reality into a manageable form for evidence-based policy Strategic Intelligence Monitor on Personal Health Systems phase 2 (SIMPHS 2)." JRC-IPTS EUR 24825

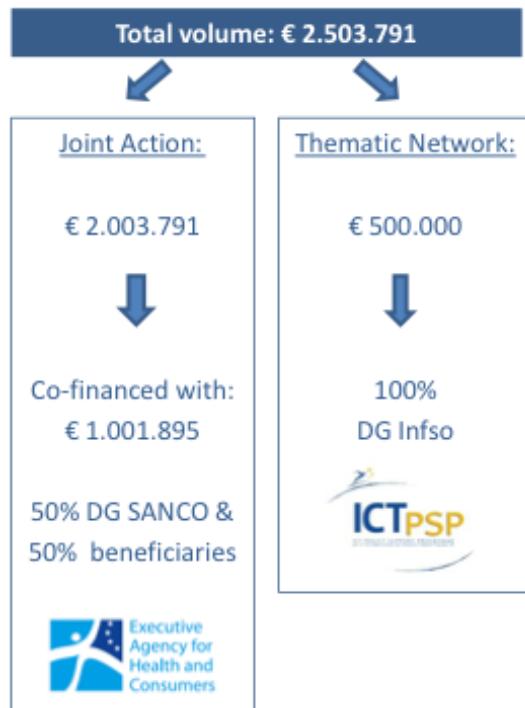
Sabes-Figuera, Ramon, and I. Maghiros. (2013) "European hospital survey: benchmarking deployment of e-Health services (2012–2013)." *European Comission*

Codagnone, C., and F. Lupiáñez-Villanueva. (2013) "Benchmarking deployment of eHealth among general practitioners. Final report." European Union. Luxembourg. Publications Office of the European Union: European Commission. Directorate-General of Communications Networks. Content & Technology.

Lupiáñez-Villanueva, F et (2018) Benchmarking Deployment of Ehealth Among General Practitioners: Final Report European Union. Luxembourg. Publications Office of the European Union: European Commission. Directorate-General of Communications Networks. Content & Technology

(currently DG CONNECT), in the following two JAs, DG SANTE increased its commitment by financing 60% of the total JA budget, the rest being paid by the Member States.

Figure 8. Financing of the eHealth Network during the eHGI JA (2012-2014)



Source: eHealth network

Overall, 25 Member States received direct EU financial support in eHealth via the **Connecting Europe Facility (CEF)**. CEF is a key EU funding instrument of the Innovation and Networks Executive Agency (INEA), aiming to promote growth, jobs and competitiveness through targeted infrastructure investment at European level, supporting interconnected trans-European networks in the fields of transport, energy and digital services. CEF funds in eHealth are used to support the European Reference Networks (ERNS) for Rare Diseases as well as supporting cross-border ePrescription and patient summary services (MyHealth@EU, ex eHealth Digital Service Infrastructure - eHDSI). The eHN guidelines are the reference for the electronic exchange of health data adopted by MyHealth@EU.

MyHealth@EU is a platform supporting the deployment and operation of services for cross-border health data exchange, meant as a move from the epSOS conceptual framework to its deployment phase. Whenever real patient data are exchanged, the NCPeH must be in conformity with the agreed principles as adopted by the eHN (Nalin, 2019).

Most Member States (22) were supported by the CEF on cross-border exchange of ePrescription and patient summary, namely: Austria, Cyprus, Czech Republic, Germany, Estonia, Greece, Finland, France, Croatia, Hungary, Ireland, Italy, Luxembourg, Malta, Portugal, Sweden, Belgium, Spain, Lithuania, Netherlands, Poland, Slovenia.

The table below summarise the indicative budget allocated to eHealth activities by the CEF during the 2015-2020 period.

Table 47. CEF Financing

year	Indicative budget spent (EUR)	Call ID
2015	7.5 million	CEF-TC 2015-2
2017	9 million	CEF-TC-2017-2
2018	5 million	CEF-TC-2018-4
2019	5 million	CEF-TC-2019-2
2020	5 million	CEF-TC-2020-2
2015-2020	31.5 million	-

Source: INEA²⁰⁶

In Annex 8.6.1, we provide an overview of potential future financial instruments that could continue to support the activities already started.

5.3.2 Activities

Since its inception, the activities of the eHealth Network have been based on the priorities set out in its **Multiannual Work Plan (MWP)**. Each JA, developed a different MWP. The box below summarises the main activities carried out during the different MWPs.

Box 51. Main activities carried out

eHGI (2012-2014)

- Development of roadmap, guidelines and formats for ePrescription, eSummary and eID

JAs eHN (2015-2018)

- Revise EU eHealth guidelines
- Propose framework for eID and NCP
- Refine eHealth European Interoperability Framework (ReEIF)
- Define m-health framework
- Evaluating global eHealth specifications

eHAction (2018-2021)

- Support of MyHealth@EU uptake and legal matters
- Take forward eID, cybersecurity
- Develop guidelines on COVID 19 contact tracing App and EU Digital COVID Certificate

Source: Author's elaboration

During **eHGI JA (2012-2014)** the **first guidelines** were produced on a non-exhaustive list of data to be included in patient's summary as well as guidelines for cross-border electronic exchange of patients' summary data set and guidelines on the interoperability of ePrescriptions.

²⁰⁶ <https://ec.europa.eu/inea/en/connecting-europe-facility>

Many of the published guidelines had to be further refined in the following JAs, such as the 2016 Guidelines on Electronic exchange of health data under the Cross-border Directive²⁰⁷ to be updated and better detailed.

The eHealth network was also supported by the work of other financed projects such as epSOS and STORK 2.0. As a result, the network contributed to the **development of the formats for ePrescription and eSummary as well as cross-border electronic identification and authentication (eID) formats**. epSOS, meaning "Smart Open Services for European Patients", was a European large-scale pilot testing the cross-border sharing of certain health data: a summary of a patient's most important health data in case of unplanned care (the patient summary) and the electronic prescription (ePrescription), while the STORK 2.0 built on the STORK framework for cross-border electronic identification and authentication (eID) of citizens and businesses in the EU and Associated Countries. STORK 2.0 allowed citizens to identify themselves across-borders by using identity-related data from authentic and reliable sources (attribute providers) or to represent other natural or legal persons, in the context of different business domains.

During the **JAséHN (2015-2018)**, most of the activities focused on supporting the implementation of **MyHealth@EU**. In total, 15 policy documents of different natures were elaborated by JASeHN with a **focus on delivering the prerequisites and key elements necessary for the establishment of the MyHealth@EU**, which was launched at the beginning of 2017. The documents provided required updates on previous guidelines, as well as proposing a framework for eID formats and National Contact Points. An important document produced by JASeHN and adopted by eHN in 2017 is the "Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth (NCPeHs) on the Criteria required for the participation in Cross-Border eHealth Information Service". According to this agreement, cross-border exchange of health data can only happen when the Member States involved enter into an agreement for this specific purpose, legally based on the national law of the respective Member States.

The governance and operating principles of the NCPeHs have been outlined in the eHN Guideline on an **Organisational Framework for eHealth National Contact Point** adopted by the eHealth Network in November 2015. The NCPeH constitutes a Member States' communication gateway providing the interface between the national infrastructure and the EU network of other Member States' NCPeH, as well as with the central EU services. The NCPeH must be recognizable both in the EU domain (with the NCPeH of other countries) and in the national domain, acting as the main interface between the two. Every NCPeH can work in two different scenarios, when a patient is travelling abroad for any reason (holiday, study, work relocation, etc.):

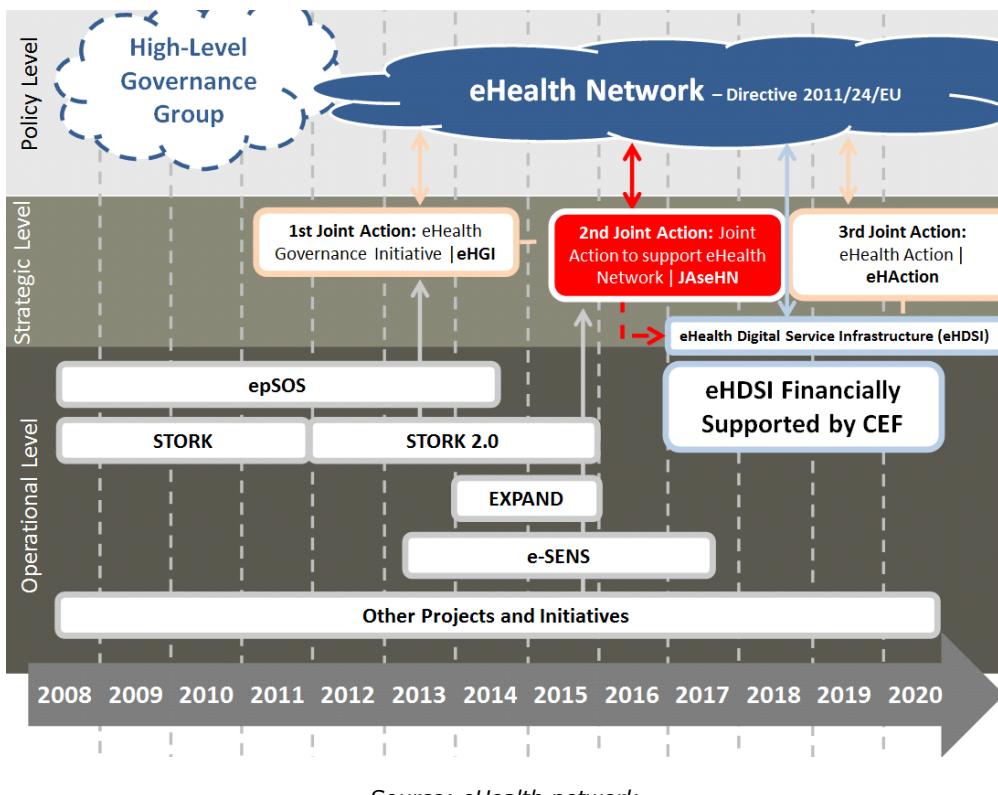
- **Country-A:** It is the Country of Affiliation, i.e., the country which holds information about a patient, where the patient can be univocally identified and where his/her data may be accessed.
- **Country-B:** It is the Country of Treatment, i.e., the country where cross-border healthcare is provided, when the patient is seeking care abroad.

Different EU Member States deployed their NCPeH in different moments, based on the MyHealth@EU NCPeH service deployment plan. These in turn are related to the national policies and strategies pursued in the area of eHealth. The MyHealth@EU was built as an infrastructure using ICT in order to enable the exchange of eHealth information services across the borders of countries within Europe. Therefore, it will be considered as the initial deployment and operation

²⁰⁷ https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20160607_co05_03_en.pdf

of services for cross-border health data exchange under the Connecting Europe Facility (CEF). The MyHealth@EU sets up and starts deploying the core and generic services, as defined in the CEF, for the Patient Summary and ePrescriptions. The generic services are the necessary implementation of data exchange at country level, the core services at EU level. Together, these enable the provision of cross-border eHealth information services. Other activities also focussed on m-health, in collaboration with the subgroup of eHN in this area²⁰⁸.

Figure 9. JAseHN overall positioning



Source: eHealth network

The main activities of **eHAction** aimed at supporting the **deployment of MyHealth@EU** (ex eHDSI)²⁰⁹, as well as other aspects on interoperability of electronic health records along the lines set out in the Commission Recommendation on Electronic Health Record Exchange Format (including national networks), cybersecurity, e-identification, capacity building, empowerment of patients via tele-health etc.

Following the break out of the COVID 19, eHealth Network was the main group that brought together Member States, supported by the Commission, to create an EU-wide digital infrastructure for mobile applications to support **contact tracing** in the EU's fight against COVID-19 as well as supporting the development of interoperable **EU Digital COVID Certificate** via an EU-wide infrastructure (entailing national infrastructures and back-end and an EU gateway).

The MyHealth@EU is the initial deployment and operation of services for cross-border health data exchange. MyHealth@EU sets up and starts deploying the core and generic services, for Patient Summary and ePrescription. The generic services are the necessary implementation of data exchange at country level, the core services at EU level. These together enable the provision of **Cross Border eHealth Information Services** (CBeHIS). The CEF, and, as of 2021,

²⁰⁸ [ev_20170509_c009_en.pdf \(europa.eu\)](https://ec.europa.eu/20170509_c009_en.pdf); [ev_20161121_c022_en.pdf \(europa.eu\)](https://ec.europa.eu/20161121_c022_en.pdf)

²⁰⁹ <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHealth+DSI+Operations+Home>

EU4Health, is the financial framework under which the MyHealth@EU initiative is carried out. The core services are set-up and deployed by the European Commission using its own resources and through calls for tender financed by CEF. The generic services are funded from the national sources and supported by grants from the CEF and, as of 2021, from EU4Health²¹⁰.

The CBeHIS is an IT tool for the exchange of health data under the CEF programme²¹¹. The role of the MyHealth@EU for Cross-Border eHealth Information Services should be to facilitate the cross-border exchange of health data between the Member States participating in the eHealth Network as recognised in the 2017 Council Conclusions on Health in the Digital Society²¹².

The exchange of health-related information has experienced a surge in the current COVID-19 crisis²¹³. In a recent Commission Implementing Decision 2020/1023, specific **rules for the cross-border exchange of data between national contact tracing and warning mobile applications as a means to combat the COVID-19 pandemic were provided**²¹⁴. Several Member States have developed mobile applications (apps) that support contact tracing and enable the users of such applications to be alerted to take appropriate action if they have been potentially exposed to the virus.

To facilitate the interoperability of national contact tracing and warning mobile applications across Member States, a digital infrastructure was developed with the support of the Commission by the Member States participating in the eHealth Network which decided to advance their cooperation in this area on a voluntary basis, as an IT tool for exchange of data. This digital infrastructure is referred to as 'the federation gateway' in the Commission's Implementing Decision 2020/1023. Implementing decision 2020/1023 lays down provisions on the role of the participating Member States and of the Commission for the functioning of the federation gateway for the cross-border interoperability of national contact tracing and warning mobile applications.

Efforts in 2021 focused on supporting the creation of interoperable **EU Digital COVID Certificates**. An EU Digital COVID Certificate is a digital proof that a person has been vaccinated against COVID-19, has recovered from COVID-19 or has a negative test result. This was based on a regulation²¹⁵, supported by free movement legal basis – article 21 TFEU, and a comitology committee (where most of the eHealth Network members have been designated). The implementing acts had been prepared by the guidelines of the eHealth Network²¹⁶.

The changes in activities carried out brought by the COVID 19 pandemic were not planned in the MWP 2018-2021. Overall, most of the effort carried out up until 2019 **focused on ensuring the setting up of the MyHealth@EU platform to run electronic cross-border health services (Patients' summaries and ePrescriptions)**. Normally, the eHealth Network carries out two meetings a year. However, during the COVID 19 crisis, weekly online meetings have been set up. Furthermore, different working groups have set-up additional meetings to discuss the different ongoing activities, especially on contact tracing, warning apps and COVID 19 certificates.²¹⁷

²¹⁰ <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Mission>

²¹¹ The Legal principles and requirements applied to CBeHIS will be stated and described in the Multilateral Legal Agreement (MLA) being prepared by the eHN Legal SG

²¹² [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XG1221\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XG1221(01)&from=EN)

²¹³ [eHealth and COVID-19 | Public Health \(europa.eu\)](#)

²¹⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2020.227.01.0001.01.ENG>

²¹⁵ [EUR-Lex - 32021R0953 - EN - EUR-Lex \(europa.eu\)](#)

²¹⁶ [eHealth and COVID-19 | Public Health \(europa.eu\)](#)

²¹⁷ Annex 8.6.3 provides a detailed description of all the activities and outputs included in the different MWPs, while Annex 8.6.4 provides an overview of the future activities.

5.3.3 Outputs

As a result of the activities described in the previous section, the main outputs delivered since the adoption of Article 14 of Directive 2011/24/EU have been the following:

Box 52. Main outputs delivered

- Development of a cross-border electronic identification and authentication (eID) approach
- Guidelines for ePrescription and Patient Summary (interoperability)
- eHealth National Contact Points
- MyHealth@EU platform
- Covid 19 contact tracing app framework and digital infrastructure
- EU Digital COVID Certificate and digital infrastructure

Source: Author's elaboration

The first years of activity resulted in the development and later update of guidelines and formats for **eID, ePrescription and Patient Summary** (eHGI JA and JAeHn). The second JA (JAeHn) also coincided with the launching of the **eHealth National Contact Points** and the **MyHealth@EU** platform which was built on the previously developed frameworks, formats and guidelines. The **MyHealth@EU** platform currently supports Patient Summary and ePrescription services. 2019 and 2020 have seen the roll-out of the first implementations in the first Member States.

As described in the previous section, the eHealth Network provided a **framework for the development of Covid 19 contact tracing apps** across the different Member States, which supported the creation of the **European Federation Gateway Service** to enable different national apps to exchange information.

Moreover, the eHealth Network provided a **framework for creating interoperable EU Digital COVID Certificates** by setting up:

- Guidelines on verifiable vaccination certificates (basic interoperability elements);
- A minimum dataset of COVID-19 citizen recovery interoperable certificates;
- A trust framework, including an EU digital infrastructure for interoperability of EU Digital COVID certificates.

By the 1st of July 2021 the EU Digital COVID Certificate will enter into application through the EU. Between the 1st of July and the 12th of August 2021 there will be a phase in period to allow Member States that are not ready to issue the new certificate to use other formats.

Annex 8.6.3 provides a detailed description of all the activities and outputs included in the different MWPs.

5.3.4 Outcomes

In terms of adoption of common secure identification and authentication system, adoption of guidelines and common requirements for personal health data (i.e. ePrescription and eSummary) and Member States' ICTs interoperability with MyHealth@EU (provision of Cross-Border eHealth Information Services), by end of 2020 only 7 countries so far reached a certain level of interoperability with MyHealth@EU. This number is below the expected target of having already 8 Member States operative by the end of 2020. The table below summarise which services are currently supported by which countries on the MyHealth@EU platform.

Table 48. eHealth services availability across EU Member States

Doctors from the countries below:	Number of Hospitals (% over total)	can access health data of citizens coming from:
Croatia	80 (100%)	Czechia (Sept. 2019), Malta (Feb. 2020) and Portugal (Feb. 2020)
Luxembourg	4 (100%)	Czechia (Jun. 2019), Malta (Dec. 2019)
Malta	1 (50%)	Portugal (Feb. 2020)
Portugal ^{218, 219}	5 (2%)	Malta (Jan. 2020)
Czechia	37 (100%)	Croatia (Dec. 2020)
Health data of citizens from the countries below:	can be consulted by doctors from the countries below, using the Patient Summary:	
Czechia	Luxembourg (Jun. 2019), Croatia (Sept. 2019)	
Malta	Luxembourg (Dec. 2019), Portugal (Jan. 2020), Croatia (Feb. 2020)	
Portugal	Malta (21 Feb. 2020) , Croatia (Feb. 2020) and Luxembourg (March 2020)	
Croatia	Malta (17 Dec. 2020), Portugal (17 Dec. 2020), Czech Republic (21 Dec. 2020)	
ePrescriptions of citizens from countries below:	can be retrieved in pharmacies in:	
Croatia	Finland (August 2020), Portugal (August 2020)	
Estonia	Finland (June 2020), Croatia (August 2020)	
Finland	Estonia (January 2019), Croatia (September 2019), Portugal (August 2020)	
Portugal ^{218, 219}	Estonia (June 2020), Finland (August 2020), Croatia (August 2020)	
Pharmacists of countries below:	Number of Pharmacies (% over total)	can dispense ePrescriptions presented by citizens from:
Croatia	1147 (100%)	Finland (September 2019), Estonia (August 2020), Portugal (August 2020)
Estonia	500 (100%)	Finland (January 2019), Croatia (March 2020), Portugal (June 2020)
Finland	386 (48%)	Estonia (June 2020), Portugal (August 2020), Croatia (August 2020)
Portugal	1 (0.03%)	Finland (August 2020), Croatia (August 2020)

Source: EC²²⁰²¹⁸ <https://www.sns.gov.pt/sns-saude-mais/cuidados-de-saude-no-estrangeiro-2/>²¹⁹ <https://www.spms.min-saude.pt/a-minha-saude-na-europa/>²²⁰ https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en

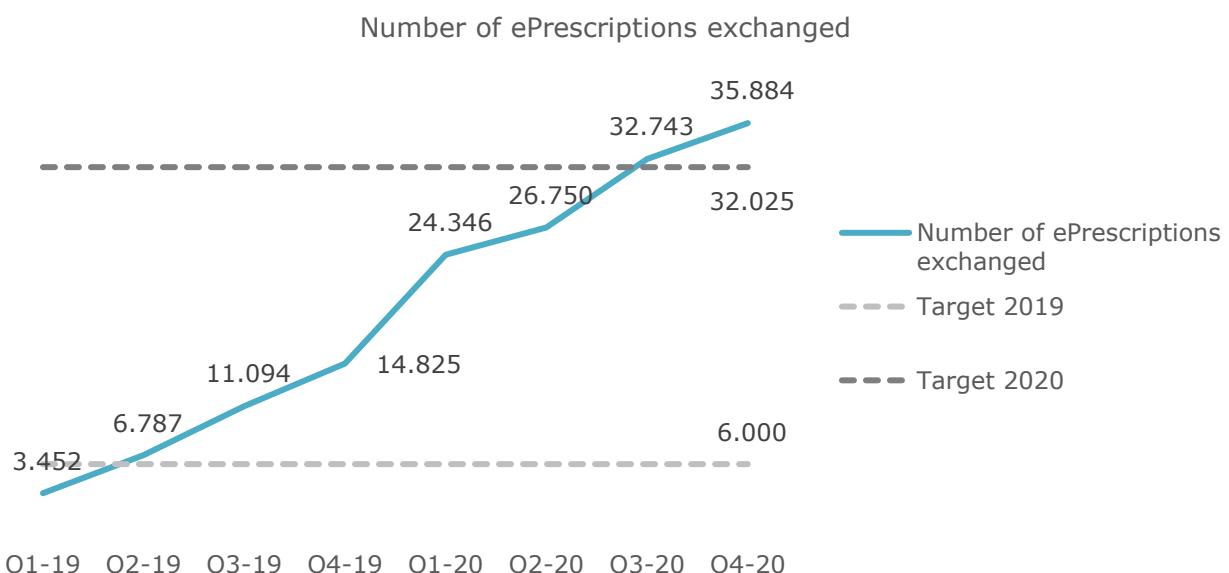
To sum up, at the end of 2020 there were 9 operational eP (A²²¹ and B²²²) services and 8 operational Patient Summary (A and B) services²²³. This number is lower than the expected target for the end of 2020, which was to have 12 operational eP (A and B) services and 20 operational Patient Summary (A and B) services.

In terms of hospitals that enabled MyHealth@EU services as countries of treatment, Luxembourg, Czechia and Croatia already provide a full national coverage. In the case of Malta, only one of the two hospitals present in the country (Mater Dei Hospital on the island of Malta) enabled the service. Nevertheless, since the other Hospital is located on the island of Gozo, where only 8% of inbound tourists spend at least 1 night, the actual coverage in terms of cross-border healthcare is potentially higher. In the case of Portugal instead, only a minority of Hospitals (5 out of 247) enabled MyHealth@EU services.

In terms of pharmacies that enabled MyHealth@EU services as countries of treatment, Estonia, Croatia and Finland are the most advanced examples in Europe with 100% (Estonia and Croatia) and 48% (Finland) respectively of pharmacies enabling the services. In the case of Portugal only one pharmacy (of the 2972 present in the country) was reported to have enabled MyHealth@EU services.

In terms of platform usage, data have been recorded as of 2019 and, as summarised in the figures below, has increased constantly year after year. Although not as many operational services as planned were set up, the overall amount of exchanges were more than initially targeted. The far majority of ePrescription exchanges (A and B) happened between Finland and Estonia, while only very few exchanges involved Portugal or Croatia. In the case of Patient Summaries, there are still relatively few exchanges and no clear pattern can be identified among Portugal, Luxembourg, Czechia and Malta.

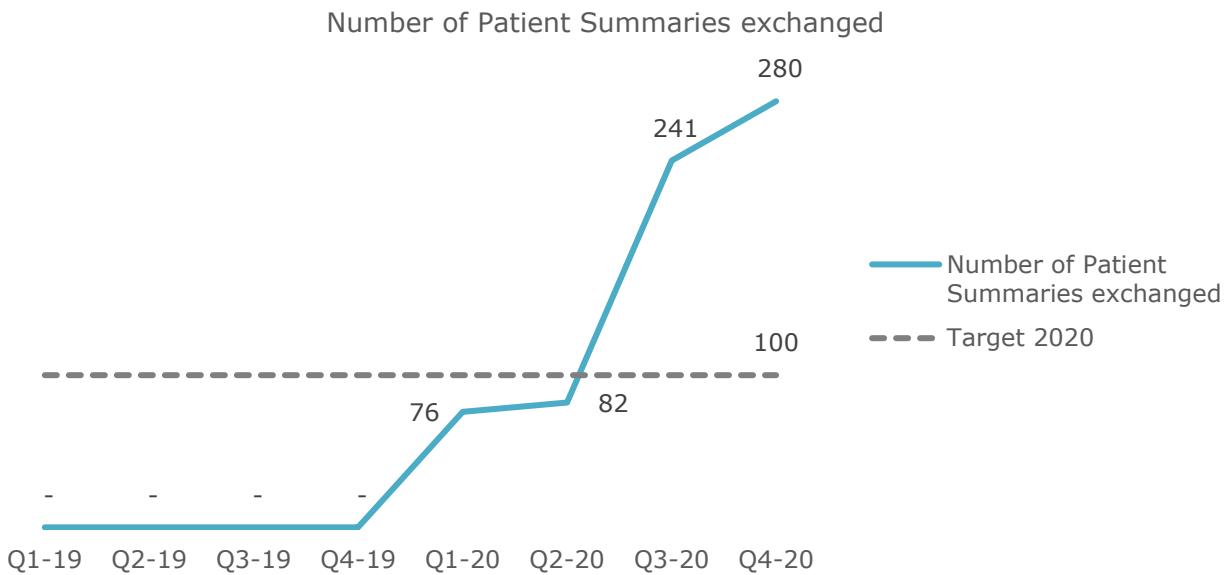
Figure 10. MyHealth@EU usage: number of ePrescription and Patient summaries exchanged



²²¹ Country of affiliation

²²² Country of treatment

²²³ Every two countries exchanging one service is considered as one operational service.



Source: EC²²⁴

Although the work on eID in eHealth is far from recent as early projects started in 2008 (epSOS & STORK), it hasn't yet made its debut in the currently operational MyHealth@EU services. At the EU level, there is no mainstream standard used, causing every identification authority to define its own implementation/usage protocol.

In terms of contact tracing apps and the interoperability across Member States, as summarised in the table below, by the end of May 2021 there were 22 apps in Europe. Of those apps, 20 were developed following the shared guidelines and can potentially support interoperability and out of them, 19 were already interoperable with the European Federation Gateway Service, which allows for interoperability across apps.

Table 49. Mobile contact tracing apps in EU Member States

Countries	App	Interoperable - is this app potentially interoperable?	Interoperable - can this app already talk to another app?
Austria	Stopp Corona App	Yes	Yes
Belgium	Coronalert	Yes	Yes
Bulgaria	Not foreseen	-	-
Croatia	Stop COVID-19	Yes	Yes
Cyprus	CovTracer-EN	Yes	Yes
Czechia	eRouška	Yes	Yes
Denmark	Smittestop	Yes	Yes
Estonia	HOIA	Yes	Yes
Finland	Koronavilkku	Yes	Yes
France	TousAntiCovid	No	-
Germany	Corona-Warn-App	Yes	Yes
Greece	Under development	Yes	-
Hungary	VirusRadar	No	-

²²⁴ https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=35210477#_ftnref2

Countries	App	Interoperable - is this app potentially interoperable?	Interoperable - can this app already talk to another app?
Ireland	COVID Tracker	Yes	Yes
Italy	Immunì	Yes	Yes
Latvia	Apturi Covid	Yes	Yes
Lithuania	Korona Stop LT	Yes	Yes
Luxembourg	Not foreseen	-	-
Malta	COVIDAlert	Yes	Yes
Netherlands	CoronaMelder	Yes	Yes
Norway	Smittestopp	Yes	Yes
Poland	ProteGO Safe	Yes	Yes
Portugal	StayAway COVID	Yes	No
Romania	exploring possible development	-	-
Slovakia	Under development	-	-
Slovenia	#OstaniZdrav	Yes	Yes
Spain	Radar Covid	Yes	Yes
Sweden	Not foreseen	-	-

Source: EC²²⁵

In terms of EU Digital COVID certificate and as summarised in the figure below. All the Member States issue and are able to verify the certificates (for vaccination, tests, or recovery) of the other Member States. Several third countries (including Switzerland, Vatican, San Marino, Turkey, Ukraine, Northern Macedonia) are connected to the gateway and the EU Member States can check in a simplified manner the COVID certificates issued by these third countries; the process is ongoing for other third countries.

²²⁵ https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en

Figure 11. Member States readiness to implement the EU Digital COVID certificate Gateway



Source: EC²²⁶

5.3.5 Impacts

The box below summarises the expected impacts associated with the outcomes (see section 5.3.4) of Article 14 of Directive 2011/24/EU.

Box 53. Expected impacts

- Patients have access to safe and high-quality cross-border eHealth products and services, improving health outcomes.
- Continuity of care for patients is ensured after treatments and/or services are provided by healthcare providers abroad, improving health outcomes.
- Increased harmonised health data for research, innovation and public health.

Source: Author's elaboration

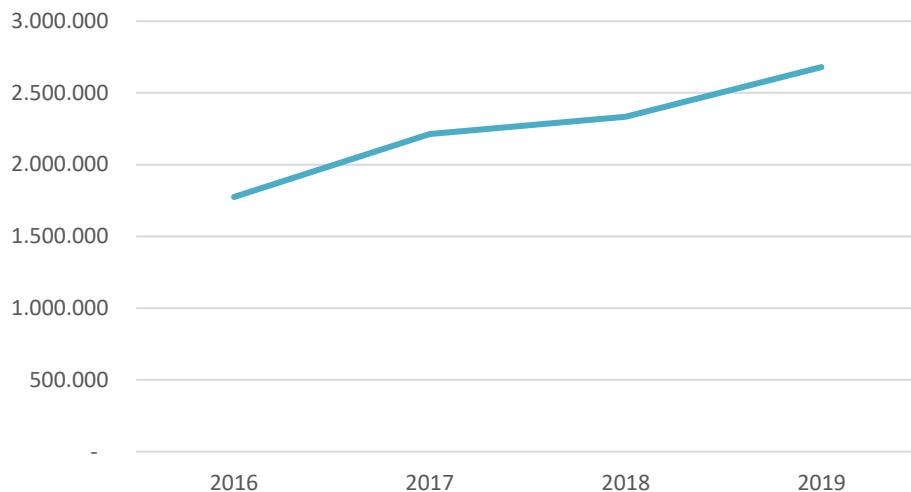
If we assess the impacts on **patient mobility**, there are three cross-border healthcare situations regulated by Directive 2011/24/EU and Regulation 883/2004 which represent potential beneficiaries from MyHealth@EU. (1) There is unplanned necessary cross-border healthcare when necessary and unforeseen healthcare is received during a temporary stay outside of the competent Member State. (2) Planned cross-border healthcare may be received in a Member State other than the competent Member State when patients purposely seek out healthcare abroad. Finally, (3) persons who reside in a Member State other than the competent Member State are also entitled to receive healthcare.

In the case of unplanned healthcare, The European Health Insurance Card (EHIC) proves the entitlement of the insured person to necessary healthcare in kind during a temporary stay in a Member State other than the competent Member State, like for example during tourism it is

²²⁶ https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

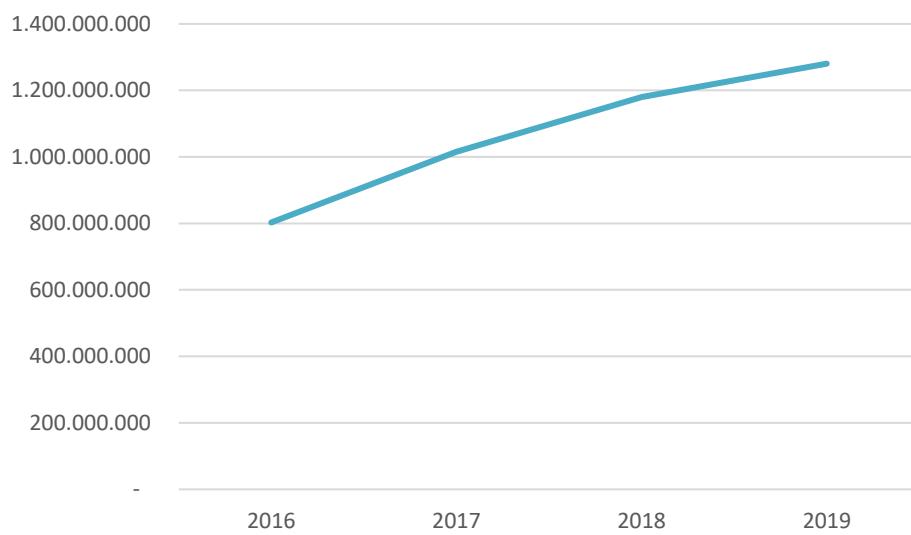
estimated that around 1.0% of tourists in Europe had unplanned care in 2019²²⁷. Furthermore, the figure below shows an overall constant increase in patient mobility across Europe in the case of unplanned healthcare. In 2019, we reached a total of 2,679,756 forms/claims across Europe, for a total amount paid by the countries of affiliation of € 1,280,450,122.

Figure 12. Total number of forms/claims received/issued by the Member States of affiliation



Source: Authors' elaboration based on the Administrative data EHIC Questionnaire of 2017, 2018, 2019, 2020

Figure 13. Total amount paid by the Member States of affiliation (in €)



Source: Authors' elaboration based on the Administrative data EHIC Questionnaire of 2017, 2018, 2019, 2020

In case of planned healthcare, the Portable Document S2 (PD S2) certifies the entitlement of the insured person to planned health treatment in a Member State other than the competent Member State. In 2019, approximately 10 out of 100,000 insured persons received a Portable Document S2 (PD S2). Among all Member States, only Luxembourg shows a rather high volume of patient mobility to receive planned healthcare in another Member State (some 13 out of 1,000 insured persons received a PD S2). The figures below presents the evolution of the total number of claims, which has remained more or less constant since 2018. On the other hand, the value

²²⁷ <https://ec.europa.eu/social/BlobServlet?docId=23857&langId=en>

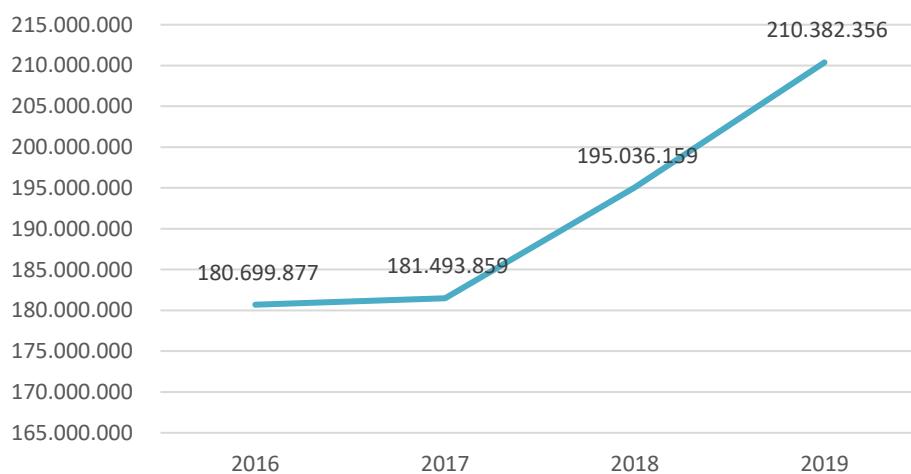
of the claim has increased, and so has the total debt owned by the Member States of Affiliation (Figure 15)

Figure 14. Total number of claims received by the Member States of affiliation



Source: Authors' elaboration based on the Administrative data EHIC Questionnaire of 2017, 2018, 2019, 2020

Figure 15. Total amount of debits owed by the Member States of affiliation



Source: Authors' elaboration based on the Administrative data EHIC Questionnaire of 2017, 2018, 2019, 2020

A 2018 report on Member States data on cross-border patient healthcare following Directive 2011/24/EU²²⁸, provides some further insights. Requests for information on cross-border care received by National and Regional Contact Points in 2017 accounted to 71,396 across the 25 NCPs providing data. While most Member States received fewer than 1,000 requests, Poland and Lithuania stand out in receiving 30,698 and 14,470 respectively. The 2017 data show an increase in requests for information since 2016, when a total of 69,723 requests were received.

As already mentioned at the beginning of this section, the European Commission estimated that almost half of the EU population has a European Health Insurance Card, and over 2 million request reimbursements yearly. In 2017, there were 17 million EU citizens living in an EU Member States other than their country of citizenship and 1.4 million cross-border workers were active in the EU.

²²⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52018DC0651&from=EN>

In its report Den Exter (2015) explains that, when available, electronic health records are often only accessible locally, or at the regional level. In terms of patients access to safe and high-quality cross-border eHealth products and services, the use of MyHealth@EU, although above the forecasted targets, is still very limited in absolute terms. So far only 7 Member States offer some kind of services on the platform. All together, these 7 countries account for 32,997,906 people which represents only 7.38% of the overall EU population²²⁹ that can access some kind of MyHealth@EU service (for more details please see Table 48).

This of course also affects the level of continuity of care for patients after treatments and/or services are provided by healthcare providers abroad. Given the relatively low level of platform usage and cross-border mobility, no major impacts on national healthcare systems were identified. According to Azzopardi-Muscat (2018), the directive did not have a major transformative effect on national health systems.

Although enabling citizens to take an active role in the management of their health was included in the last JA, the impact of article 14 on the access of patients to their electronic health records was limited as no outputs impacting this area were produced. As a result, only a handful of countries provides electronic formats when implementing Article 4.2 (f) and Article 5 (d) of the Directive 2011/24. Only 4 Member States have rules to provide digital access to a copy of the medical record/s for patients affiliated to their healthcare system seeking cross-border healthcare in another Member States (Croatia, Czechia, Greece and the Netherlands) and Finland is planning to implement such rules over the upcoming three years.

Table 50. Rules to provide digital access to a copy of the medical record/s for patients affiliated to your healthcare system seeking cross-border healthcare in another Member States

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	Yes	Luxembourg	No
Cyprus	No	Malta	No
Czechia	Yes	Netherlands	Yes
Denmark	No	Poland	No
Estonia	No	Portugal	No
Finland	Planned	Romania	No
France	No	Slovakia	No
Germany	No	Slovenia	No
Greece	Yes	Spain	No
Hungary	No	Sweden	No
Ireland	No		

*Planned within the next three years

Source: Author's elaboration based on country survey results

²²⁹ EUROSTAT 2019 data

In terms of rules to provide digital access to a copy of the medical record/s of received treatment/s for patients affiliated to a different healthcare system that used cross-border healthcare in their Member States, only three countries provide such rules (Germany, Greece and the Netherlands) and three are planning to do so over the coming three years (Czechia, Finland and Poland).

Table 51. Rules to provide digital access to a copy of the medical record/s of received treatment/s for patients affiliated to a different healthcare system that used cross-border healthcare in your Member States

	Yes/Planned*/No		Yes/Planned*/No
Austria	No	Italy	No
Belgium	No	Latvia	No
Bulgaria	No	Lithuania	No
Croatia	No	Luxembourg	No
Cyprus	No	Malta	No
Czechia	Planned	Netherlands	Yes
Denmark	No	Poland	Planned
Estonia	No	Portugal	No
Finland	Planned	Romania	No
France	No	Slovakia	No
Germany	Yes	Slovenia	No
Greece	Yes	Spain	No
Hungary	No	Sweden	No
Ireland	No		

*Planned within the next three years

Source: Author's elaboration based on country survey results. For a country by country overview, please refer to the Country Fiches.

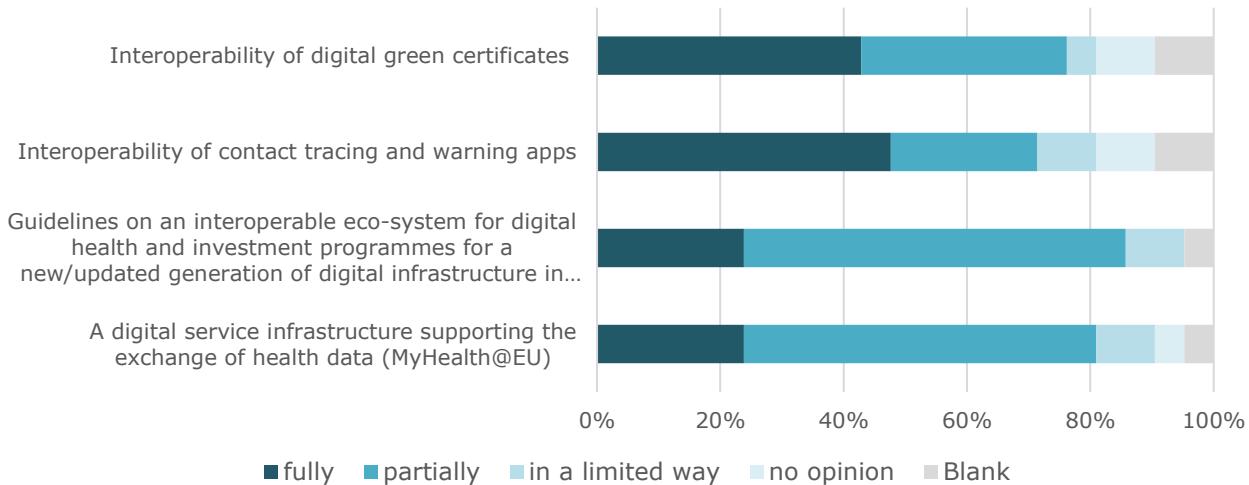
While the activities carried out in the field of contact tracing apps resulted in 18 interoperable apps being developed, pick-up rates of these apps have been limited. Probably the main factor explaining this difference relies in a different privacy culture and in a trust deficit towards contact tracing apps. A 2020 survey on the perception of contact-tracing across 19 countries²³⁰ found that in countries such as Germany and France 21% and 25% of respondents respectively would not provide personal information. In Vietnam, only 4% of participants replied the same.

In terms of EU Digital COVID certificate, in June and July, over 230 mil certificates have been issued. This number is higher in countries that decided to use the COVID certificates for access to different events or activities. The certificates issued in different Member States can be used in others, including for national use (such as access to different socio-cultural events). Once implemented, the EU Digital COVID Certificate will be accepted in all EU Member States and will help to ensure that restrictions to free movement of persons currently in place can be lifted in a coordinated manner.

²³⁰ https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Global_ICL-YouGov-Covid-19-Behaviour-Tracker_contact-tracing_20200821_vF%5B1%5D.pdf

When eHealth Network members were enquired about the achieved impacts, different opinion emerged (see figure below). More than half of the respondents believed that they only partially achieved a digital service infrastructure supporting the exchange of health data (MyHealth@EU) as well as guidelines on an interoperable eco-system for digital health and investment programmes for a new/updated generation of digital infrastructure in Europe. While almost half of the respondents believed that they fully developed interoperability of contact tracing and warning apps as well as of EU Digital COVID Certificates.

Figure 16. Self-assessed results of Article 14 (a)



Survey Question: In your opinion, to what extent did the eHealth Network achieved the above-mentioned objective of Article 14 (a) set out in the legislation "work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare", by delivering: (n=19)

Source: Author's elaboration

5.3.6 Other EU policies

Since 2011, digital needs and policies responses have also evolved. As flagged in the list of documents summarised in the box below, new advances in technologies, AI and big data have also created new needs to be able to retrieve better and faster harmonised data to advance research, prevent diseases and provide personalised healthcare. The current COVID-19 pandemic is a reminder of how useful and potentially impactful these data can be not only from a medical point of view, but also from a policy responsiveness perspective. New citizen-centric policies are also highlighting the need to **ensure citizens' secure access to and sharing of health data across borders** as well as enable citizens to take an active role in the management of their own health data, including in the area of e-health, m-health and telemedicine.

Box 54. Other EU policies and relevant EU documents

- The eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century.
- The Digital Single Market Strategy: eHealth (Telemedicine) is mentioned under the section Boosting competitiveness through interoperability and standardisation.
- The communications under the Digital Single Market Strategy: there were four European Commission Communications published on 19 April 2016 of which in particular the last two included actions on eHealth:
 - Digitizing European Industry;
 - The European Cloud Initiative;
 - The EU e-Government Action Plan 2016-2020;
 - Priorities of ICT standardisation for the Digital Single Market.
- Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society
- Recommendations of the Commission's study on Big Data in Public Health, Telemedicine and Healthcare.
- eHealth Network mHealth sub-group report on suggestions for future work.
- The Data Strategy and the White Paper on Artificial Intelligence are the first pillars of the new digital strategy of the Commission.
- Data Governance Act (proposal)

The **eHealth Action Plan 2012–2020-Innovative healthcare for the 21st century** was probably the first policy document to shape the eHealth Network activities. The eHealth action plan from 2012 evaluated the development of eHealth and defined the main objectives. In 2012, despite the economic crisis, the telemedicine market was booming, at an annual rate of 18.9% between 2010 and 2011. However, the complexity of the European legal framework was already a heavy burden. Most of the obstacles hampering the deployment of eHealth at the time are still not addressed:

- lack of awareness of, and confidence in eHealth solutions among patients, citizens and healthcare professionals;
- lack of interoperability between eHealth solutions;
- limited large-scale evidence of the cost-effectiveness of eHealth tools and services;
- lack of legal clarity for health and wellbeing mobile applications;
- inadequate or fragmented legal frameworks including the lack of reimbursement schemes for eHealth services;
- high start-up costs involved in setting up eHealth systems;
- regional differences in accessing ICT services, limited access in deprived areas.

The four actions defined to address these barriers were

- Achieving wider interoperability in eHealth Services
- Supporting research, development, innovation and competitiveness in eHealth
- Facilitating uptake and ensuring wider deployment of eHealth
- Promoting policy dialogue and international cooperation on eHealth at global level

The first action, interoperability, was supposed to be led by the eHealth network. Through their expertise both on technical aspects and at a Member States level, they had as an outcome

several guidelines and projects such as the ReEIF (the Refined eHealth European Interoperability Framework) and epSOS addressing the legal issues.

eHealth innovation support was included in the “Health, demographic change and well-being” of Horizon 2020 in the following areas: 5P medicine, data valuation for diagnosis, health promotion and cost-effective healthcare.

Based on the work carried out within the **Digital Single Market Strategy**, and more specifically the **EU e-Government Action Plan 2016-2020** communication as well as the communication on the **priorities of ICT standardisation for the Digital Single Market**, in 2018 the EC published a **Communication on Digital Transformation of Health and Care**. The communication identified three priorities:

- **Citizens' secure access to their health data**, including across borders, enabling citizens to access their health data across the EU;
- **Personalised medicine through shared European data infrastructure**, allowing researchers and other professionals to pool resources (data, expertise, computing processing and storage capacities) across the EU;
- **Citizen empowerment with digital tools** for user feedback and person-centred care using digital tools to empower people to look after their health, stimulate prevention and enable feedback and interaction between users and healthcare providers.

The proposal for a Regulation on European data governance (**Data Governance Act**), is the first of a set of measures announced in the 2020 European strategy for data. The instrument aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. It will be complemented in the health domain, the act seeks to improve the conditions for data sharing in the internal market, by creating a harmonised framework for health data exchanges, the **European health data space (EHDS)**. So far the EHDS has not been established yet.

Some of the changes brought by these later policies have somewhat been reflected in the MWPs of the different JAs supporting the eHealth network over the years. Furthermore, in the box below, we provide a list of European Grants carried out in the area of eHealth. Of those, the most relevant ones are the ones already discussed in section 5.3.2 (i.e. epSOS, and STORK). Other relevant grants representing the European Commission efforts to develop digital health, both for primary and secondary use and eHealth/mHealth are:

Box 55. Other relevant EU projects

- PHIRI (Population health data exchange)
- InfAct (EU health information system infrastructure)
- ImpleMentAll (eHealth implementation)
- EOSC-Life (Collaborative space for digital biology)
- EJP-RD (Rare disease digital ecosystem)
- HealthyCloud (health R&I cloud)
- Do->IT (big data health research)
- EHDN (Health Data Network)
- InteropEHRate (health data interoperability)

Source: Authors' elaboration

5.3.7 Member States digitalisation and interoperability and the impact of the eHealth Network

The Directive 2011/24/EU recognises the problems related to interoperability. For instance, recital 56 states that: "technological developments in cross-border provision of healthcare through the use of ICTs may result in the exercise of supervisory responsibilities by Member States being unclear and can thus hinder the free movement of healthcare and give rise to possible additional risks to health protection. Widely different and incompatible formats and standards are used for provision of healthcare using ICTs throughout the Union, creating both obstacles to this mode of cross-border healthcare provision and possible risks to health protection. It is therefore necessary for Member States to aim at interoperability of ICT systems". However, the Directive was put forward with a very strong logic of national competence (mostly from a perspective of health than a perspective of digital single market) and focussed on national measure mostly. Therefore, recital 56 states that: "this Directive therefore should recognise the importance of the work on interoperability and respect the division of competences by providing for the Commission and Member States to work together on developing measures which are not legally binding but provide additional tools that are available to Member States to facilitate greater interoperability of ICT systems in the healthcare field and to support patient access to eHealth applications, whenever Member States decide to introduce them". However, the article 14 (2)(a) is quite wide: "work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare".

A detailed analysis of the digitalisation at national level has been carried out by Empirica and Open Evidence and has shown that 80% of countries have passed national legislation on electronic health records (EHRs), regulating data safety and technical security measures less than five years ago. Logging of health data processing was not found to be mandatory in nine countries.

While 26 countries generally provide their citizens with access to EHR data by law, only 20 states have recorded by law that citizen access must be possible independent of place and technology. 43% or 12 countries indicate that their citizens are not entitled to choose which healthcare professional or other party can access their EHR. Often general practitioners act as 'data gatekeepers', allowing additional parties to access a patient's EHR, while in other countries the technical readiness of health data systems is not yet advanced enough to realise this option.

Most countries specify conditions for alteration and archiving of electronic health data but only around one third allow patients to correct data entered in their EHR by themselves. Two thirds of countries detail measures for technical interoperability and exchange measures in their legislative framework. 18 study countries indicate that data sharing of EHRs across national borders is permitted by law.

Uniformly, one-third of study countries indicate that their eHealth policy is not integrated into general healthcare policy and that it does not contain planning measures for patient safety and quality of care, suggesting that eHealth policy is somewhat isolated in the respective countries. In terms of awareness actions and citizen information campaigns, 23 countries claim to actively promote EHR system uptake and utilisation.

In terms of alignment between national and EU-level eHealth efforts and resources, the data show a mixed picture. Out of 28 study countries, nine indicate to not refer to EU-level guidelines and documents on the Patient Summary and ePrescription/eDispensation in national policy documents and 19 do not refer to these resources in legislation documents. Only seven countries

lack a standalone technical interoperability strategy. 17 countries have implemented an interoperability strategy focusing on semantics through a national terminology centre.

Organisational level and financial investments: measures to support

Access to health information for citizens has been facilitated nationwide in 17 countries, while six countries report ongoing pilot projects. Patient access to health data is not a reality in three countries.

Access to EHR data via an online portal is by far the most common mode of access. Another four countries report offering mobile access while two countries still use paper print-outs (note that multiple answers could be valid for a single country). 19 countries provide citizens the opportunity to have their health data corrected, only three countries go as far as allowing citizens to delete EHR contents. In 18 countries citizens are able to manage EHR data access on a document level. Viewing test results is the most common EHR service, followed by prescription and appointment services.

Overall, most countries report dedicating an appropriate budget and human resources to implementing the national eHealth strategy and create new institutions that take over the role of the executing body.

While 27 countries have set-up a competent authority for eHealth, this competent authority does not evaluate or assess eHealth impacts – be it social or economic impacts – in around one-third of countries.

Moreover, cybersecurity and data protection expertise are not present in these authorities in seven countries, while two countries have added the expertise to the relevant competent authority after the launch of the “Recommendation on an European Electronic Health Record exchange format” in February 2019. 24 countries report that competent authorities aim to facilitate semantic and technical interoperability, but only slightly more than half of all countries also publish guidelines, maintain terminology archives, or perform mapping activities to international standards.

Translating international standards into local language is the most widely offered service by the competent authorities for eHealth (18 countries), followed by providing national extensions (17 countries). 16 countries report contributing to international working groups developing standards and competent authorities in 15 countries undertake licensing activities. Other services are offered by less than half of the study countries.

Of all 28 study countries, only 16 have created a forum that is comparable to the National Digital Health Network envisaged by the EU Commission. The most frequently engaged stakeholders in this forum are the national eHealth Network representatives followed by the NCPeH, organisations responsible for semantics and technical interoperability, Public Health authorities, national Medical Drug Agency and the competent authorities for Telehealth and controlling the quality of healthcare. Authorities for Genomics, AI and Data Protection are less frequently engaged as stakeholders. 19 countries report granting public funding to local infrastructure projects for EHR systems. Financial penalties or subsidies coupled to the implementation of EHR systems are deployed in 16 states, however, 18 states report mandatory adoption timeframes for new standards. Nine and eleven countries, respectively, do not regularly assess the state of EHR interoperability and conclude policy-relevant actions from such assessments. Exactly half of all countries claim to promote the eHDSI/MyHealth@EU nationally.

Security and access

Digital signatures are the most common authentication practice in Europe for patients and healthcare professionals, followed by two-factor authentication. In 6 Member States, EHR systems are supported by distributed ledger technologies (DLTs) and these countries have also been actively researching further applications of DLTs in the health data space. 3 Member States have not implemented a framework with technical and cybersecurity-related requirements for health professional identification and authentication in EHR systems. 5 Member States report not to employ the identification means according to the eIDAS regulation. While 3 Member States lack unique patient identifiers, 2 do not have such identifiers for healthcare staff.

More than two-third of countries make use of consistent encryption and a security-by-design approach to prevent cyber-attacks. However, only one-third of countries train healthcare personnel in the area of cyber-security risks. Penetration testing is a common practice among study countries, but 3 Member States do not perform well on this indicator.

Only three countries have not yet established a single point of contact for the security of network and information systems covering the health sector.

Semantic Interoperability

From all patient summary sections available, over two-thirds of study countries have made clinical terminology standards mandatory for diagnoses, medications, billing purposes and procedures. Only half of countries report mandatory standards for immunisation and allergy data. Most EU countries have not yet implemented a terminology server. While only around one-third of countries have implemented SNOMED CT or LOINC, 6 Member States have not implemented either of these terminologies. Less than a third of Member States have implemented eHealth DSI resources.

Technical Interoperability

Patient summaries exist in two-thirds of all study countries and are most frequently accessed via an online portal, but only several Member States can share patient summaries. ePrescription services exist in two-thirds of all study countries and are most frequently accessed via online portals. However, eleven countries are still using paper printouts. In 20 countries the majority of GPs is connected to EHR systems and routinely uses the services offered, followed by pharmacies in 19 countries. Laboratories, hospitals and specialist practices are connected to HER systems in over 20 countries, but the routine use is recorded in only 15 countries.

Level of actual use of interoperable EHRs

The pharmacy sector in Europe is almost completely connected to national EHR systems in over 50% of study countries and service-related data is being exchanged between pharmacies and EHRs. 5 Member States do not have yet an ePrescription system in place. 4 Member States do not have a fully functioning EHR system and only few advanced countries have the home care sector connected to such a national system. Some of the Nordic and Baltic countries are found to have the highest level of EHR use across categories overall. 6 Member States show an overall low level of use across all EHR data types, whereas the Nordic countries and Estonia have the highest level of use.

In general, the more advanced countries show a similarly high level of use among health professionals. Countries with a higher level of use in one category typically have higher levels of use in the remaining two categories, too. 3 Member States are more focussed on the primary care sector. In most countries, the amount of clearly structured electronic health data remains low.

Use of EHRs and big data for early warning and surveillance as well as digital diagnosis (COVID-19) While the vast majority of the countries have created a system to collect epidemiological surveillance data, only slightly more than half the countries receive this data in standardised fashion. Whilst around 10 Member States can automatically generate surveillance data, even some advanced countries do neither have a standardised messaging service nor mandatory electronic surveillance software in place.

Impact of eHealth Network on national digitalisation

The study quoted above also inquired into the impact of the eHealth Network on the national digitalisation, based on discussions with representatives of national authorities, including in the eHealth Network. It also looked into the way the Commission Recommendation on Electronic Health Record Exchange Format impacted on the national EHR development in different Member States.

The importance of the European eHealth Network and its related initiatives and resources is rated very important by four respondents and another 15 claim it be important to national interoperability developments. At a closer look, the data suggest that while only a few Member State representatives are strongly convinced of the importance of the eHealth Network, not a single respondent claims it to be unimportant. In terms of impact, two respondents estimate it to be weak, but a total of 16 respondents found it had a high or very high impact on national EHR interoperability developments. When asked to rate the importance and impact of the provision of specific standards and specifications in general, respondents answer more positively. Several indicators analysed whether Member States had adopted the eHealth Network guidelines on patient summaries and ePrescriptions from 2016. The impact opinion-poll matches quite well with reality: around half of the countries have adopted the guidelines.

The number of Member States which assign high importance and strong impact to the general provision of eHealth Network guidelines is higher than the number of countries which have actually adopted guidelines from the eHealth Network. 40% or the equivalent of eleven countries attribute a very high importance to this fact, while another eight countries regard this as important (amounting to a total of 19 countries or almost 70%). Asked about the Recommendation's impact on national developments, respondents' estimates are more conservative: "very high" is selected only four times, while "high" is selected ten times by the recipients. Three respondents even claim it had a weak or very weak impact. The remaining eleven representatives attribute a somewhat strong or weak impact to the adoption of the EHR Recommendation.

In terms of policy implications for interoperability of electronic health records, a more salient finding is that the perceived importance of the European eHealth Network is greater than its perceived impacts. While a large number of respondents generally perceive it as very important to be provided with international guidelines on the implementation of, e.g., ePrescriptions for cross-border exchange, a smaller number of respondents find the eHealth Network's initiative and resources very important or highly impactful. A similar interpretation can be made for the perception of the EHR Recommendation itself.

The study hence confirms that the eHealth Network has had a limited impact on the barriers to access to health data for both primary and secondary purposes. Because of the non-binding nature of eHealth Network guidelines, which recommends the uptake of interoperability standards, the guidelines have had little impact in the Member States. The data collected show furthermore that, whilst progress has been made, electronic health records are not a reality across the whole of the EU, and many patients cannot easily access and use them, or transmit their data between healthcare sectors or providers. However, whilst the study focussed more on

the electronic health records, it is very likely that the impact of the eHealth Network would have been considered higher in areas covered by COVID: digital contact tracing and warning apps and especially the EU Digital COVID certificates, where a strong legal basis for the EU-wide infrastructure was put in place.

5.4 Analysis and evaluation

5.4.1 Effectiveness

To measure the effectiveness of the eHealth Network, in this section we compare the outcomes and impacts presented in section 5.3.4 and 5.3.5 respectively with the objectives set out in Directive 2011/24. The analysis tries to capture to what extent the outcomes of the activities carried out addressed the underlying objectives.

In terms of specific objectives, the activities carried out under Article 14 developed a common secure identification and authentication system of patients and healthcare providers, as well as specified semantic, legal and technical requirements for the standardisation of patient summaries and electronic prescriptions. These guidelines and standards were included in the developed MyHealth@EU platform (supported by the CEF programme programme and EU4Health as of 2021), which is used to run the electronic cross-border health information services (so far ePrescriptions and Patient Summary, more services to be added, such as images and image reports, laboratory results and discharge letters). While the platform can facilitate the exchange of patients' health data across borders to enable continuity of care and patient safety across borders, its uptake has been so far limited to 7 Member States. Since many Member States so far have not implemented the developed standards and guidelines, lack of interoperability of digital health services systems remains one of the major obstacles for realising access to safe and high-quality cross-border healthcare. According to the experts interviewed, one of the reasons behind the relatively low adoption of the platform lies in the voluntary nature of the network and the voluntary participation in MyHealth@EU that had no hard mandate towards Member States. Nevertheless, in quantitative terms, the level of information exchanged on the platform was higher than the forecasted target (see section 5.3.4). As the amount of Member States up taking the platform will increase, so will the effectiveness of having the platform. **Ensuring a high up-take level of the platform will increase the impact in terms of patients' access to safe and high-quality cross-border eHealth products and services, as well as continuity of care for patients receiving cross-border healthcare or benefitting from free movement within the EU.**

The eHealth network did not directly support patients in accessing their health data in other Member States. As of today, only 4 Member States have rules to provide digital access to a copy of the medical record/s for patients affiliated to their healthcare system seeking cross-border healthcare in another Member States and 3 Member States provide digital access to a copy of the medical record/s of received treatment/s for patients affiliated to a different healthcare system. However, MyHealth@EU, which allows healthcare professionals (in the country of destination) to access patient's data support, as well as its future development of (such as access of patients to their health data) can support these evolutions. The lack of eHealth Network activities in the area mixed with the lack of Member States priority in the area resulted in a very low level of effectiveness.

When it comes to the support of national digitalisation, interoperability and access of patients to their health data, progress has been made at national level since 2011, but this cannot be linked directly to the work of eHealth Network (except for contact tracing apps and especially EU Digital COVID certificates), as not all the Member States implemented eHealth Network guidelines at national level. Even though the General Data Protection Regulation has specific provisions on

the access of data subjects to their data and portability of this data, eHealth Network took limited measures at EU level to implement these provisions. However, some measures were taken at national level. For instance, 26 countries generally provide their citizens with access to electronic health record data by law and 20 states have recorded by law that citizen access must be possible independent of place and technology, whilst patient access to health data is not a reality in three countries. 18 countries indicate that data sharing of EHRs across national borders is permitted by law. 27 countries have a digital health authority, with different tasks related to interoperability, security, data protection, tele-health and m-health. 24 countries report that competent authorities aim to facilitate semantic and technical interoperability. Also, some Member States took into account the Commission Recommendation on Electronic Health Record Exchange Format, supported by the eHealth Network through investment guidelines²³¹, as well as the recommendation of 3 June 2021 on National Digital Health Networks²³², developed with the support of eHAction. However, the members of the eHealth Network had, for a very long time, a political profile (representatives of the ministries of health). eHealth Member States Expert Group had concentrated in the past the technical expertise, focussed on eHDSI/MyHealth@EU. Only recently, with the creation of the semantic and technical subgroups, the technical expertise has been brought forward more strongly, allowing for technical discussions on digitalisation to feed directly the main decisions of the eHealth Network. The discussions on standards and specifications have been focused on eHDSI/MyHealth@EU and only recently started to systematically cover the national interoperability of electronic health records fuelled by the Commission Recommendation on Electronic Health Record Exchange Format. Whilst a subgroup of the eHealth Network on m-health recommended to set up an assessment framework that would support member States in their work in this area, the temporary character of this group did not ensure a proper follow-up, reflected in guidelines of the eHealth Network in this area. Overall, as the eHealth Network guidelines were voluntary, their impact on national development were rather limited and the effectiveness of eHealth Network was low.

Innovative use of health data has been developed in the fight against COVID (i.e. Contact tracing apps, EU Digital COVID Certificates), stimulating the use of health data for policy marking. This had a positive impact on the public health of the Union, providing crucial new tools in times of health crisis. These tools also helped to lift Member States temporary restrictions to the free movement of people, supporting the protection of an EU citizenship right. The digital infrastructure on contact tracing apps was anchored in an implementing decision of the eHealth Network and was based on a voluntary approach (not all the MS developed such apps and 2 developed centralised approaches). However, the eHealth Network managed to bring important coordination at EU level and changes at national level, done in rather similar way in several Member States. Such national and European transformation was even more visible for the EU Digital Covid Certificate, which had a strong legal basis (a regulation based on free movement of persons). Given the very high level of expertise brought forward in the semantic and technical subgroups of the eHealth Network and the coordination role of the eHealth Network, the Member States managed to deploy in few months an EU wide infrastructure, with a strong national rollout. The Commission also provided a strong support for EU interoperability. Therefore, on actions related to crisis, one can say that the effectiveness of the eHealth Network was very high.

In terms of secondary use of data, no actions have been taken to boost secondary use of health data in research. In this area the eHealth Network was not effective. Some eHealth Network members justified the lack of action in the area as the result of several factors. On the one side,

²³¹ [ev_20190611_co922_en.pdf \(europa.eu\)](https://ec.europa.eu/eurostat/documents/20190611_co922_en.pdf)

²³² [eHAction_eHN-Recommendations-National-Digital-Health-Networks- -for-adoption_19th-eHN.pdf](https://ec.europa.eu/health/sites/default/files/documents/eHAction_eHN-Recommendations-National-Digital-Health-Networks- -for-adoption_19th-eHN.pdf)

the prioritisation of developing ePrescriptions and patients' summary together with the infrastructure to run such services across Member States (MyHealth@EU) took most of the capacity not allowing to focus on other topics. On the other side, up until 2020 the issue was lacking political support at Member States level and given the voluntary structure of the network, that represented an obstacle to moving forward in the area. The digital health agencies, represented in the eHealth Network had in many cases a national mandate focussed on the use of data for healthcare. As mentioned in section 5.3.6, while no activities on secondary use of data were carried out by the eHealth Network, other EU initiatives did support the re-use of health data for research and innovation. A relevant example is the work carried out in the field of rare diseases²³³. Therefore, some impacts have been reached in the area, but they were not linked to effective eHealth Network activities.

Since the Directive has been adopted in 2011, at the national level the need for better management of data for policy making, research and innovation has been recognised by some Member States with the set-up of different (data permit authorities, national health institutes etc.) new national institutions (i.e. Findata, French Data Hub, etc.) with this exact objective. As further explained in section 5.4.4, the need for action in this area brought the European Commission to initiate a new Joint action to help Member States and the Commission in developing sharing of health data for public health, treatment, research and innovation in Europe (THEDAS). With the setting up of a European Health Data Space, THEDAS future activities are likely to impact the amount and availability of harmonised public data for research, innovation and public health across the Union. Within the scope of secondary use of data, it is important to note that the introduction of the 2016 GDPR brought not only a framework to guarantee safe processing of personal data, but also provides a shared framework for secondary used of data. Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (on the basis of Union or Member State law) have been considered by the GDPR (Article 6(1)(e) GDPR).

5.4.2 Efficiency

To measure the efficiency of the eHealth Network, in this section we analyse the activities carried out and presented in section 5.3.2 with the input and resources provided and explained in section 5.3.1. The analysis tries to capture to what extent the actions carried out under Article 14 have been realised in a cost-effective way, including MyHealth@EU.

As a general rule, the benefits of EU interventions are expected to justify the costs they generate, although those who bear the costs do not always reap the benefits. This is a common situation in the health domain, where final beneficiaries are supposed to be citizens and patients. Furthermore, due to a lack of accounting of man-days and other inputs, it was not always feasible to quantify exactly the costs sustained by certain stakeholders. Nevertheless, in this section we try to identify which factors are driving these costs/benefits and how these factors impacted the eHealth Network activities.

In terms of costs, the major contributors to eHealth Network activities have been the European Union and the different Member States. Within the European Commission, the Directorate-General for Health and Food Safety (DG SANTE) was a major contributor to the different Joint Actions. The table below summarises DG SANTE financial contribution to the Joint Actions supporting the eHealth Network since its creation.

²³³ https://ec.europa.eu/info/research-and-innovation/research-area/health-research-and-innovation/rare-diseases_en

Table 52. Financing of eHealth Network Joint Actions

	DG SANTE	Member States	Total JA budget
eHGI JA (2012-2014)	1,001,895 EUR (50% of total budget)	1,001,895 EUR (50% of total budget)	2,003,791 EUR
JAs eHn (2015-2018)	2,400,000 EUR (60% of total budget)	1,600,000 EUR (40% of total budget)	4,000,000 EUR
EHAction (2018-2021)	2,699,989.67 EUR (60% of total budget)	1,799,985.38 EUR (40% of total budget)	4,499,963.46 EUR

Source: European Commission

Overall DG SANTE provided more than €6 Million in JAs since 2012. DG SANTE has increased greatly its contribution from the first to the second JA while its contribution has increased only slightly from the second to the third JA. Member States have also co-financed a sizable percentage of the budget for the first and second JA. The JAs budgets covered:

- Support for development of policy documents to support the different priority areas identified in the MWPs
- The dissemination of content produced within Member States and Stakeholder Groups;
- The dialogue with relevant EU eHealth stakeholder groups and standardisation organizations;

The financial inputs that contributed to the work of the eHealth Network, were not limited to the already mentioned Joint Actions and support provided from Health programme (and EU4Health), but included also the Connecting Europe Facility which supported the development of the MyHealth@EU and some EU grants which supported the initial elements used for the set-up of primary data standards and interoperability. For the purpose of this analysis we excluded other grants and projects that were linked to eHealth in Europe, but not to Article 14 specifically. In addition, Health programme (and EU4Health as of 2021) and DG SANTE ensured the eHealth Network secretariat, the preparation and reimbursements of eHealth Network meetings and its subgroups.

DG CONNECT supported the development of the MyHealth@EU platform via the Connecting Europe Facility (CEF). The CEF (2015-2020) is the main financial framework under which the **MyHealth@EU initiative** was carried out. Between 2015 and 2020, INEA, the Innovation and Networks Executive Agency managed approximately 31.5 million EUR in funds for eHealth activities. In this context, the eHealth Network guidelines for electronic identification, ePrescriptions and Patients Summary are the reference for the electronic exchange of health data adopted by MyHealth@EU. Furthermore, the work conducted by the eHealth Network on semantics, interoperability and setting up National Contact Points for eHealth (NCPeH), constituted a relevant input to the roll out and functioning of the infrastructure. . As of 2021, this funding will move under EU4Health.

The CEF funds have contributed to develop and run the MyHealth@EU platform at national and EU level by supporting the:

- National grants for setting up National Contact Points for eHealth
- Management and governance of the platform
- Requirements and specifications
- Configuration services

- Terminology services
- Test and Audit services
- NCPeH Reference Implementation
- Operations orchestration
- Hosting

The Directorate-General for Research and Innovation (DG RTD) is responsible for managing the financial instruments implementing the main research and innovation programmes (i.e. FP7, H2020, Horizon Europe, etc.). Over the years, these grants co-financed several relevant projects for the implementation of article 14 of Directive 2011/24. Before the setting up of CEF, different projects already started to build the groundwork to deliver digital cross-border eHealth services, by defining eID formats, as well as formats and frameworks for the digital exchange of Patient Summaries and ePrescriptions. The most relevant projects within the scope of this research are summarised in the following table:

Table 53. Relevant EU projects

	Topic	Budget	EU contribution
epSOS	Patient Summary and e Prescriptions	38,008,793 EUR	17,999,000 EUR
STORK & STORK 2.0	Cross-border authentication and identification (eID)	26,453,042 EUR 18,655,793 EUR	13,073,335 EUR 8,762,939 EUR
EXPAND	Deploying cross-border eHealth services	989,988 EUR	989,988 EUR
e-SENS	Deploying cross-border eHealth services	27,358,005 EUR	13,678,995 EUR
Total		111,465,621 EUR	54,504,257 EUR

Source: European Commission

As highlighted in the previous two tables, Member States have also financially contributed to JAs and projects. Furthermore, according to the stakeholders involved in the study, particular extra effort was required by the 7 Member States that are already interacting with MyHealth@EU to join the platform. Furthermore, there are significant differences across countries that needs to be considered. According to the three-country analysis of den Exter et al. (2015), Croatia, Netherlands, and Italy have taken considerable steps to realize the Cross-Border Health Care Directive's (2011/24) aims. Each of the three countries have taken regulatory steps to reach these objectives from a mainly "*copy and paste*" approach (Croatia) to a "highly complicated multilevel decision-making process" (Italy). The paper seems to suggest that countries with complex regionally different healthcare systems (i.e. Italy, Germany and Spain) may encounter greater barriers to adopt the developed tools and guidelines. Similar comments were provided by the experts interviewed in this study.

Some financial support to some Member States has been provided by the Directorate-General for Structural Reform Support (DG REFORM). DG REFORM works closely with Member States and offers technical support to design and implement structural reforms. These are targeted, time limited projects, which are usually directed towards one Member States and take place at the request of a Member States. Technical support includes context specific study visits and best practice exchange between the Member States/Regions. Digital health is one of the areas where REFORM provides technical support (i.e. the 2021-2027 Croatian eHealth Strategic Development

Plan and Croatian eHealth Business Implementation Plan 2021-2022). Bulgaria, Belgium, Estonia, Greece and Slovenia also receive support from REFORM to develop their eHealth strategies and future proof ICT governance frameworks. Czechia received technical support for the creation and implementation of the national eHealth centre. DG REFORM is also involved in the work regarding eGovERA, which is the eGovernment Enterprise Reference Architecture. eGovERA has also developed expertise in the area of eHealth, with help from Czechia and Ireland in the last months. For example, under the Multi-annual Financial Framework 2014-2020, around EUR 1 billion were allocated for digital health from the European Regional Development Fund (ERDF) and almost **EUR 12 billion** have been negotiated by the Commission and Member States under Recovery and Resilience Facility (**RRF**) in this area.

On top of these financial inputs, additional human capital has been invested to ensure the execution of the eHealth Network activities. This includes especially the time spent by national experts and representatives, that on top of participating in semi-annual meetings, also organised and carried out their work in thematic sub-groups. Unfortunately, upon request no information was provided on an estimation of these costs. As a result, it was not possible to gather evidence on the estimation of the overall Man-Days (MD) invested by the different Member States, but all stakeholders were unanimous in noting that the commitment varied greatly among members, hinting that some Member States invested far more than others. Furthermore, according to eHealth Network members, more sub-groups and frequency of meetings and activity was carried out since the start of the COVID 19 pandemic. As summarised in the figure below, a total of 254 online meetings have been organised since the start of the COVID 19 pandemic. Considering an average of 1h per meeting and the participation of one representative per Member States, we can estimate around 857.25 MD invested since the start of the pandemic until June 2021 on meetings alone (without considering the investments carried out nationally to produce and sponsor the different digital infrastructures and applications).

Table 54. Number of meetings carried out by the eHN during 2020 and 2021

Meetings	Joint Controller + Tech	Technical WG – COVID19 Mobile Tracing Apps	Coordinated Actions – Covid-19	Communication group	Technical IOP Subgroup	Business rules task force	Aviation and technical SG	Semantics	DCC Piloting Community	TOTAL /month
January 2021	5	4	5	1	X	X	X	2	X	17
February 2021	4	4	4	X	X	X	X	2	X	14
March 2021	5	6	7	X	X	X	X	5	X	23
April 2021	5	4	4	X	6	X	X	1	5	25
May 2021	2	2	5	X	6	7	2	2	4	30
June 2021	4	3	5	X	9	X	1	2	5	29
TOTAL 2021	25	23	30	1	21	7	3	14	14	138
TOTAL 2020					116					116
TOTAL eHN Meetings 2020 + 2021										254

Source: European Commission

The voluntary cooperation structure of the network resulted in different levels of commitments and investments from Members that could be justified by different national political priorities as well as different level of readiness to adopt the developed tools and guidelines.

If we look at the countries that already implemented the MyHealth@EU platform such as Finland and Estonia, they already had very **digitalised healthcare systems** (see section 5.2). On top of that, the population of both countries is concentrated in the capital regions of Helsinki and Tallinn respectively. Separated by the 65-kilometre-wide Gulf of Finland, the twin-city region of Helsinki-Tallinn is already a **highly integrated region** with relevant mobility flows across the gulf. These pre-existing conditions are likely to have played an important role not only in gathering the political support needed to adopt the MyHealth@EU platform, but also to be the two regions with the highest frequency of exchange of cross-border data. Furthermore, as highlighted by Portuguese representatives, having Portugal already a **centralised national health data system**, made it easier (and relatively cheaper) for the country to adopt all the standards required to uptake the MyHealth@EU platform compared to countries such as Spain, Germany and Italy with regional systems that already present interoperability issues within the countries.

Although the MyHealth@EU infrastructure is up and running, as seen in section 5.3.4 its adoption by Member States is so far limited to 7 countries²³⁴ compared to the target of 8 (and more in 2021). Nevertheless, the exchanges on the platform have outreached the predefined targets for 2019 and 2020. Compared to the 2011, Member States have now at their disposal a platform to exchange health data (ePrescription and eSummary) with other Member States in a secure and trustworthy manner. As more Member States will join the platform, more beneficial the tool will be for the countries that have already implemented it.

Data on EU citizens' use of the rights granted under the Directive are too old (2017) and predating the launch of the MyHealth@EU platform. The data showed no significant growth or reduction over the three previous years. Furthermore, even if available, data for 2020 and 2021 are likely to be biased due to the limited mobility of EU citizens resulted by the COVID 19 pandemic. Net of external factors, **limited commitment by Member States within the framework of a voluntary cooperation structure played a big role in limiting the effectiveness of the investments carried out in the area since 2011**. The COVID 19 pandemic brought a change in policy focus and commitment by Member States. The amount and quality of activities conducted within a short timeframe in 2020 and 2021 in the field of EU Digital COVID Certificate, are a proof to the fact that when there is political convergence and support among the different stakeholders of the voluntary network and, ideally, a stronger legal basis, the efficiency of the eHealth Network increase greatly. From the beginning of 2020, the eHealth Network developed guidelines that supported the development of 19 interoperable contact tracing apps, as well as the development of the EU Digital COVID certificate, whose launch is foreseen by July 1st, 2021. It is important to note that in the case of the EU Digital COVID certificate, the initiative was legally supported by a regulation²³⁵, while in the case of the MyHealth@EU platform, no regulation on standardisation and harmonisation was proposed, everything was carried out within a voluntary cooperation framework. This was probably another factor that increased the effectiveness of the activities carried out for the EU Digital COVID certificate.

The table below summarises the different costs and benefits by stakeholder group:

²³⁴ 2020

²³⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130>

Table 55. Overview costs and benefits

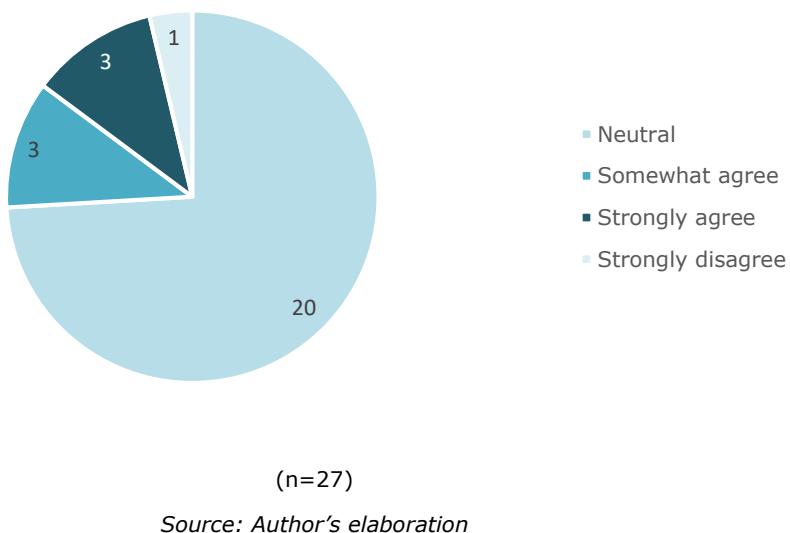
European Commission		Member States		Citizens		HCP		
	Qualitative	Quantitative / monetary	Qualitative	Quantitative / monetary	Qualitative	Quantitative / monetary	Qualitative	Quantitative / monetary
Costs								
Direct costs	Low	DG SANTE: €6 million in JAs since 2012 € 1.2 mil - Health budget for meetings organisation MD:NA	Low	€4.4 million in JAs since 2012 MD: NA	-	-	-	-
Indirect costs	Medium	INEA: € 31.5 million DG RTD: € 54,5 million	Medium	DG RTD projects: € 57 million Implementation of MyHealth@EU solution: NA Development of tracing apps: NA	-	-	-	-
Benefits								
Direct benefits	Better monitoring of cross border healthcare.	-	Better monitoring of cross border healthcare. Better public policy and monitoring (tracing app and digital pass)	-	Patients have access to safe and high-quality cross-border eHealth products and services, improving health outcomes.	Total number of forms/claims received/issued	Continuity of care.	Total number of forms/claims received/issued
Indirect benefits	Support freedom of movement across the Union	Number of temporary restrictions in the different Member States	-	-	Lifting of temporary restrictions of free movement.	Number of temporary restrictions in the different Member States	Less administrative burden.	-

Source: Authors' elaboration

It is important to highlight that, when enquired, none of the eHealth Network members was able to quantify the costs and benefits provided by the participation to the network, although the majority believed the network to be run in a cost-efficient manner. Future administrative procedures to participate to the eHealth Network activities should improve the accounting of the different costs (i.e. MD, national investments, etc.) to allow for a better ex-post estimation of the costs carried out.

When Member States were enquired about the extent at which the eHealth Network support contributes to a more cost-efficient development of cross-border digital health resources, the far majority did not have any strong position. Positive feedback came mainly from smaller Member States as well as Member States that have engaged more with the Network and have pushed for stronger national healthcare digitalisation policies. The figure below summarises the results of the survey.

Figure 17. To what extent do you agree that the eHealth Network support contributes to a more cost-efficient development of cross-border digital health resources



5.4.3 Relevance

To measure the relevance of the eHealth Network, in this section we analyse to what extent the objectives set out in the Directive 2011/24 were relevant with regards to the needs identified (see section 5.1).

All the objectives identified in Box 48 remain relevant as interoperability issues are still present. The MyHealth@EU platform has been implemented so far by only 7 Member States. Therefore barriers to exchange patient's health data across borders to enable continuity of care and patient safety across borders are still present.

In terms of patients' access to data, as highlighted in Table 50 and Table 51, ad-hoc electronical medical record/summary of the treatment received supporting the continuity of care across borders have rarely been implemented, nor is required by article 4 and 5 of the Directive 2011/24. While in 2011 it was chosen not to impose an obligation to issue electronic copies of medical records/treatment received, a potential revision of the Directive could consider the possibility to foster more remote access to medical record in the context of cross-border healthcare.

At the same time, whilst eHealth Network issued guidelines supporting the implementation of the Commission recommendation on European Electronic Health Record Exchange Format and national interoperability, their voluntary status limited their impact on national interoperability. This area should be taken forward in the future European Health Data Space, especially in order to support the creation of a digital single market in the health sector.

The recent COVID 19 pandemic has highlighted more than ever the relevance and need of a more integrated and interoperable European eHealth system. Facilitating the exchange of patients' health data across borders to enable continuity of care and patient safety across borders remains highly relevant. In terms of semantic, legal and technical requirements for the interoperability of eHealth improvements have been made. The MyHealth@EU platform is up and running and is able to support cross-border transfer of health data (ePrescription and patient summary) using a common secure identification and authentication system.

In the future, the same platform especially after the eID system will be integrated could be used to support other health services and enhancing accessibility to new cross-border digital health services such as tele-medicine, tele-health, tele-monitoring.

Nevertheless, the current lack of wide-spread adoption of the MyHealth@EU platform limits its results. The voluntary nature of the eHealth Network as defined in Article 14 may have negatively impacted the uptake at national level of the tools and standards developed. On the other hand, according to the different stakeholders interviewed, the network has represented the first step in facilitating the cooperation and exchange of information across Member States, although the level of participation was subject to the national political priority on the topic.

The use of common standards for health data transferred across borders through one platform could potentially also be relevant in the future to better grasp new technologies such as the use of Big Data and Artificial Intelligence in the field of healthcare. Currently these options remain uncertain (see chapters 3 and 4).

Supporting the pooling of the EU's data resources and to facilitate their use for research and health policy remains a major need that the eHealth network was not able to address. Not only enhancing secondary use of data (Article 14(b)(ii) of the Directive 2011/24) remains a major need, but further reflection is needed on how to coherently address this issue with the different EU policies implemented. To ensure better secondary use of data, some Member States have set up in the last years different governance structures and strategies for managing health data. The need to enhance secondary use of data resulted in the 2019 announcement of the Commission's work towards creation of a European Health Data Space²³⁶, which is supported by the ad-hoc THEDAS joint action. Secondary use of data solutions being developed under TEHDAS would help promote the use of health data for research, which would support research for the improvement of healthcare, taking away current existing barriers for the secondary use of health data.

5.4.4 Coherence

To fully exploit the potential of exchanging health data across borders, it is essential to ensure health data quality and that the various sources of health data (e.g. electronic health records, different registries, various IT or digital tools) are able to "talk" to each other. This requires technical and semantic interoperability between the different infrastructures and IT systems. Interoperability and security are essential parts of a digital single market. However, the activity of the eHealth Network concentrated mostly on cross-border aspects and its guidelines. Being

²³⁶ https://ec.europa.eu/health/ehealth/dataspace_en

of voluntary nature, they had a limited impact on the national interoperability and data quality, impacting on the possibility of providers of digital health services to offer their goods and services in other Member States, but also on the possibility of people having access to their data and portability of this data between healthcare providers (in line with the provisions of the General Data Protection Regulation). Even if this access and portability is ensured in many cases at national level, the approach, standards and specifications are different between different Member States, which impacts on the cross-border provision of digital services and products. Under the European Health Data Space, more efforts are needed in order to ensure a real digital single market for health sector and allow patients and citizens to have access to their data and interoperability of the data.

So far, the activities carried out under Article 14, resulted, among other things, in the development of the MyHealth@EU platform. The platform is currently able to run core primary use of data services (ePrescriptions and Patient Summary). Nevertheless, the low pick up rate highlights a certain lack of coherence with national health policies and priorities. Furthermore, the provisions of Article 14 also include the objective of supporting the innovative use of health data for secondary purposes. As already discussed, so far the majority of the activities only focused on primary use of data while fewer activities were carried out in the field of secondary use of data also because in some cases the institutions involved in the eHealth Network may have not been the best suited to do so. Furthermore, contrary to the guidelines set forward in the eHealth Action Plan 2012–2020-Innovative healthcare for the 21st century, limited activities have been conducted in the field of telehealth beyond the documents of eHAction, while in the field of mHealth, the eHealth Network set up a temporary working group, which delivered important recommendations, including on guidelines for evaluating tele-health applications. However, their follow-up was limited at the end of the mandate of this group. However, the COVID-19 pandemic brought an increase of the activities in the area of m-health (contact tracing apps and EU Digital COVID Certificates). This shows a certain lack of internal coherence as the tasks focused only on certain objectives, namely primary use of data.

As highlighted in chapter 4, there are different governance structures and strategies for managing health data in the Member States, with a particular focus on re-using data for research purposes. These include national agencies or bodies authorized to grant permits for the use of data already collected for another specific purpose, as well as any other mechanisms for providing access to health data for research and public policy purposes, including by means of initiatives to further enhance data altruism. Chapter 4 outlined thirteen data governance bodies at a Member States level as well as one in the UK. Even though the list is not exhaustive, it describes the main bodies that currently have a central role for providing access to health data for research, often existing in parallel to other bodies and data controllers that are in place.

Meanwhile, in 2020 DG SANTE conducted preparatory work, through a series of workshops and a study²³⁷ to support a framework for the primary and secondary use of health data in the Member States, the European health data space (EHDS), particularly through:

- a mapping of how the GDPR is implemented in the health sector in the different countries, including an overview of the legal and technical modalities applicable to health data sharing for primary and for secondary uses in the EU countries
- an overview of the existing governance structures for secondary use of health data in the EU countries
- recommendations for possible actions, legislative and non-legislative, at EU level to facilitate health data sharing across the EU for primary and for secondary uses

²³⁷ https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf

As a result, in February 2021 the Joint Action TEHDAS initiated its activities to support the European Commission to set up the EHDS. TEHDAS support focuses on developing principles for the cross-border secondary use of health data. TEHDAS partners include some of the identified new national agencies specialised in secondary use of data. This is coherent and complementary to the activities carried out so far under Article 14 on primary use of data and eID as the combined activities can support the development of the EHDS.

Nevertheless, the evolution of national agencies specialised in secondary use of data and data permit authorities has increased the number of actors that needs to be engaged to ensure the development of an EHDS. The current structure of the eHealth network was not able to promote cooperation between Member States in the field of secondary use of health data, nor was it able to engage with these new institutions. Therefore, to ensure the implementation of the European Health Data Space in its entirety a different structure should be developed to ensure the coordination on secondary use of health data (see chapter 4).

In terms of secondary use of data, it is also important to notice how many other EU projects (see Box 55) provided relevant inputs in the area, although their activities were often disentangled by eHealth Network activities. Ad-hoc activities carried out under the different JAs ensured that eHealth Network outputs where coherent with GDPR regulation (work carried out on eID), ensuring that citizens have control over their own personal health data.

As part of the JASeHN, an entire work package was dedicated to Global cooperation and positioning. As a result several deliverables have been produced in the field of mapping international eHealth specifications and good practices as well as organising meetings with the WHO and the OECD.

According to the interviews carried out, some stakeholders such as Insurances, MedTech or Pharma flagged that they were not invited to monitor and provide input to eHealth Network activities in a systematic way, although they represent key players in the supply of healthcare. However, such stakeholders have been invited in several meetings of the eHealth Network in the past years.

5.4.5 EU added value

Under the principle of subsidiarity (Article 5 Treaty on European Union), and in areas of non-exclusive competence, the EU should only act when the objectives can be better achieved by Union action rather than action by the Member States. Furthermore, as stated in Article 168 of the Treaty on the Functioning of the European Union, EU action must complement national policies and encourage cooperation between Member States. EU intervention contributes only where Member States cannot act individually or where coordination is the best way to move forward. While EU countries define and deliver their national health services and medical care, the EU seeks to complement national policies by means of its Health Strategy²³⁸ to:

- prevent illness/disease by promoting healthier lifestyles;
- facilitate access to better and safer healthcare;
- contribute to innovative, efficient and sustainable health systems;
- deal with cross-border threats;
- keep people healthy throughout their lifetimes;
- harness new technologies and practices.

²³⁸ https://eur-lex.europa.eu/summary/glossary/public_health.html

While looking at activities and results, we assessed changes which can reasonably be argued are due to the EU intervention, over and above what could have been expected from national actions by the Member States. In many ways, the evaluation of EU added value brings together the findings of the other criteria to assess the performance of the EU intervention in setting up the eHealth network.

According to Azzopardi-Muscat et al. (2018) the impact of the directive varies between countries and is smaller in countries where a large degree of adaptation had already taken place in response to the European Court of Justice Rulings²³⁹. Nevertheless, most of the reforms analysed did not address eHealth issues. Most reforms include a heightened emphasis on patient rights and the adoption of explicit benefits packages and tariffs. Countries may be facing increased pressure to treat patients within a medically justifiable time limit. The implementation of professional liability insurance, in countries where this did not previously exist, which may also bring benefits for patients. Lowering of reimbursement tariffs to dissuade patients from seeking treatment abroad has been reported in Poland (Azzopardi-Muscat et al., 2018). In some cases, the reforms implemented at national level also took into account the EU evolutions, the standards and specifications, but not in a systematic manner.

If we only consider eHealth and the cross-border exchange of health data for healthcare, it would be hard to imagine the development of a platform such as MyHealth@EU without EU intervention. According to the different experts interviewed (external experts as well as some eHealth network members), Member States showed different level of involvements in the different eHealth Network initiatives. The up-take rate of the platform by early adopters reflects this. In terms of interoperability and eID, countries with regional healthcare systems (i.e. Spain, Germany, Italy), still suffer from lack of national interoperability and would have seen the EU level interoperability neither as a priority nor as an opportunity to foster national interoperability within the country. Furthermore, given the relatively low level of cross-border patients, compared to national patients, when it comes to developing formats for ePrescriptions and Patient Summary some countries would have had less incentive to factor in the interoperability across the EU. This would have likely resulted in sustained lack of interoperability.

Having an established network also played an important role in reacting quickly to the COVID 19 pandemic by setting up common standards for contact tracing app and COVID certificates. The COVID 19 pandemic stressed even more the need to coordinate and ensure better flowing of health data across Europe.

The lack of activities by the eHealth Network in the field of secondary use of data provides an example of lack of coordination among Member States. As Member States stated to develop ad-hoc agencies, EU coordination was not contemplated until the setting up of the TEHDAS group.

When it comes to secondary use of health data, the involvement of new ad-hoc national agencies and data permit authorities will be crucial to develop better data usage for research and policymaking. TEHDAS has already started this process. A potential solution could be to have two different networks, one focusing on primary use of data and involving the stakeholders currently addressed by the eHealth Network and the second one focusing on secondary use of data and involving data permit authorities as well as national data agencies. The two networks would need to be interconnected to ensure lack of duplication and common use of certain tools and formats such as eID. Together, the two networks would provide the two pillars on which to build European Health Data Space, ensuring the control of citizens over their own personal health

²³⁹ The analysis was carried out in seven EU Member States. Namely: Belgium, Estonia, Finland, Germany, Malta, Poland and The Netherlands.

data and the use of data for medical diagnosis, public health and research. However, attention should be paid to the extent that the TEHDAS replicates the same path taken by the eHN.

6. Conclusions and recommendations

6.1 Digital health products and services

The recommendations on policy options have been built around the 5 main following needs that should be addressed to foster the digital health single market. The different options which are presented for each need are not mutually exclusive.

6.1.1 Establish labelling/certification/authorisation guidance for digital health services and products

Users should be able to enjoy products that do not harm patient's health and that provide at least equivalent benefit to pre-existing options. Through an action of EU legislation, labelling to support certification or authorisation, the EC has the opportunity to initiate a true single market for digital health solutions, as a first step towards unifying the perspectives on the provision of digital health services. Such guidance is intended to provide faster market access, availability of European-wide digital health solutions, better offerings and lower costs.

In order to avoid overlapping, such rules should apply to all digital health services and products regardless or not they are covered by the MDR or the AIA framework. These rules, labelling and authorisation procedures should ensure complementarity with the current regulations, addressing aspects such as interoperability, access of users/patients to data, portability and re-use of data as well as some additional security and quality aspects as far as they are not covered by MDR or AIA. The new approach shall feed into the reimbursements/procurement decisions rather than being a pre-condition for putting the product or service on the market (for products covered by MDR/AIA) and it should include (1) apps, (2) diagnosis and treatment software, (3) patient portals and personal health data spaces, (4) teleconsultation software and (5) electronic health records,

Option 1 Introduce a quality label for digital health products and services to build trust and support decision-making, A label, based on technical criteria and quality criteria, is a way to start building trust among users, in order to progressively set the use of products and services in a cross-border context, prior to establishing functional reimbursement mechanisms. The quality criteria to include in such a label could rely on the work carried out on mobile health through the mHealth hub and under the standard ISO/CEN 82304-2. It could for instance encompass the following areas: medical safety, usability, security/protection of personal data, cybersecurity, technical quality, reliability, quality of the service (including societal benefits). The context, the purpose of use and the area they apply to could be specified through a framework for better categorisation. The work on mobile health should be extended to telehealth products and services to encompass a broader scope (taking the examples of digital health assessment in Belgium, Germany or France).

It should be noted that a labelling on security and data protection will mean to meet the certification requirements under GDPR to become an approved GDPR label. Furthermore, in order to avoid overlapping, such rules should apply the most possible to both MDR and AIA products and services (ensuring complementarity with the aspects analysed under these frameworks), as well as to non-MDR and non-AIA products and services and should include the following digital health devices: (1) apps, (2) diagnosis and treatment software, (3) patient portals and personal health data spaces, (4) teleconsultation software and (5) electronic health records.

This labelling should cover criteria on (1) Medical safety, (2) Usability, (3) Security of personal data, (4) Technical quality, (5) Quality. In the technical criteria could be covered identification/authentication and interoperability, access of users/patients to data, portability

and sharing of this data. The labelling should only cover technical quality including interoperability for the MDR products. For the non MDR products and services, the labelling should cover more aspects. The quality aspects would ensure for non-medical devices to provide transparency for users, especially on health risks/benefits. For electronic health records, as well as the interoperability of medical devices/wellness apps with the electronic health records, the standards and specifications laid out in the Commission Recommendation on Electronic Health Record Exchange Format can be the minimum common denominator/starting point. It should be noted that a work on a label is already to be developed under Horizon Europe call²⁴⁰ and could support this option.

The label would be introduced at EU level, with criteria defined by the EU level governance body dealing with primary use of health data, in collaboration with digital health bodies, medical devices/HTA bodies, healthcare professional representatives, and patient associations. It would be implemented by national digital health bodies or could be delegated to third parties. This labelling could be communicated and adopted as guidelines or legislation. It would be established in complementarity to other certification and authorisation schemes without being a certification per se (e.g. under Medical Devices Regulation, horizontal AI framework, etc.), guiding towards digital health products (telehealth, mHealth) to be reimbursed or not, without specifically referring to reimbursement. It should be used with the main following purposes: (1) providing a user-facing label for consumption decisions, with easily accessible and readable information in a transparency logic towards users (healthcare providers and patients) and (2) gathering information to narrow reimbursement decision-making by the HTA bodies,. It will for instance support healthcare providers when recommending the best services, with a clear view on the assessment of their development, their trustworthiness and their efficiency regarding the benefits brought to the patients.

Option 2 Set up a mechanism to provide and maintain the quality label In addition to option 1, a quality labelling scheme with a dedicated mechanism could be set up to establish and manage labelling, to monitor and improve continuously the criteria included in the quality label under option 1 for the non-MDR and non-AIA products and services (for all criteria) or MDR/AIA products and services (for technical criteria including interoperability, access of patients/users to their data, portability and sharing of this data, some security aspects, etc). The bodies dealing with digital health or other bodies/private entities (such as Medappcare in France) recognised by the bodies dealing with digital health at national level could take this responsibility for non-MDR products and services and only on the technical aspects including interoperability, access of users/patients to data, portability and sharing of this data for the MDR products and services, in order to bring together the MS in order to agree on relevant quality labels. Trust would be established with this health authority supporting the inclusion of digital health services in a certified "library". The existing notified bodies would still bear the responsibility and take action for quality, safety aspects of the medical devices. For MDR products, the safety aspects would remain analysed by the notified bodies, however, the interoperability, portability, sharing of data and access of users/patients to data (and some security aspects) criteria should be added based on decisions taken at EU level, would be evaluated by national digital health bodies and would ensure transparency for HTA bodies.

Option 3 Introduce an assessment framework for digital health products and services. An assessment framework issued at EU level should use the existing guidelines to be used among Member States to support certification/authorisation of both non-MDR and non-AIA products and services, as well as MDR and AIA products and services. These guidelines should be translated

²⁴⁰ HORIZON-HLTH-2021-IND-07-03 Promoting a trusted mHealth label in Europe: uptake of technical specifications for quality and reliability of health and wellness apps [Funding & tenders \(europa.eu\)](https://ec.europa.eu/funding_tenders/europa.eu)

into assessment frameworks for the different product categories. To do so, the level of maturity of the frameworks for the different product categories should be assessed, since personal health data spaces and patient portals seem less mature. Such a framework would be based on specific criteria for eHealth (including AI) such as quality and interoperability, access of users to data, portability and re-use of this data, requirements for the manufacturers of digital health services and products, with a wider scope and a higher level of compliance than labelling under option 1. The definition of such a framework will be carried out in collaboration with digital health agencies/bodies, with medical devices/HTA bodies not to overlap with existing rules and responsibilities, it should include patients and HP representatives in the process to ensure the services outcomes are fit for purpose.

The framework shall only be addressed to non-MDR and non-AIA services and products, as well as to MDR and AIA products and services, it will introduce an assessment focused on the context of use -as the value of telehealth and mobile health services mainly relies on the way it is used and integrated in health and care processes-, as well as clinical benefits and cost savings. Such an assessment should be complementary with current assessments, with a need to avoid any overlap with requirements in certification as well as to best fit digital services and products lifecycles. For products and services falling under MDR and AIA frameworks, the MDR and AIA could be a starting point for practical purposes, eHealth assessment should be closely linked to reimbursement (and not a condition for putting the products and services on the market), keeping the objective to converge on evidence requirements among Member States in order to move towards common assessment methods and, to some extent, decision making processes.

However, it should be noted that adding a new assessment framework could increase fragmentation if the same product/service is subject to several different frameworks. Thus, its governance and collaboration with HTA bodies is of utmost importance to ensure relevance and visibility.

Option 4 Give EU validity to codes of conduct approved by a data protection authority and serving as a baseline. A specific code of conduct regarding the use of telehealth and mobile health will allow both to support trust among users and to guide self-certification. In such code of conduct, privacy will be a central item and could rely on the EC Green Paper on mobile health, or existing code of conducts (such as from the WHO/EC, the EDPB) or similar tools such as a Data Ethics Framework (which is used in the UK).

The Code of Conduct could include the suggestions from the WHO: (1) User's consent, (2) Purpose limitation and data minimisation, (3) Privacy by design and by default, (4) Data subjects' rights and information requirements, (5) Data retention, (6) Security measures, (7) Principles on advertising in mHealth apps, (8) Use of personal data for secondary purposes, (9) Disclosing data to third parties for processing operations, (10) Data transfers, (11) Personal data breach, (12) Data gathered from children.

Option 5 Support the inclusion of the assessment framework in current certification/authorisation schemes and support public-private partnership. In addition to option 3, the certification/authorisation framework defined at EU level could be included in the current certification/authorisation schemes through binding legislation, relying on existing governance bodies under option 2 (medical devices/HTA bodies, bodies dealing with primary use of health data...) which would provide a certification/authorisation for the digital health products that are reimbursed, especially for those provided cross-border. It should include both MDR and non-MDR products and services, with MDR products and services subject to areas not covered by MDR, to avoid overlapping. The bodies dealing with digital health or other bodies at national level would be involved to cover both technical standards (e.g. interoperability between tele-health/m-health solutions, other digital health services and products and electronic health

records, access of users to their data, portability and sharing of this data) and quality standards. Bodies or market organisations recognised by the national bodies could provide a certification/label to the manufacturers of digital health services and products that comply with quality and technical requirements. The schemes should allow for an assessment of a digital health solution in one country against a specific set of requirements determined at European level (which could be similar to those under option 1) completed by specific national requirements, allowing for the re-use of the documentation and a mutual recognition of mechanisms between Member States, thus ensuring the scale-up of services at an international level. However, for the products and services subject to MDR/AIA frameworks, such certification would be complementary and would feed into the information provided to HTA bodies.

Furthermore, the bodies will hold the responsibility to guarantee the implementation of innovative, risk-based and fit-for-purpose models that are tailored to the unique needs of software products and that support innovation while also ensuring safety and effectiveness. Their activity could also be completed on organizational maturity, since HTA bodies analyse technical quality and readiness of tools and services, not the organisational readiness of the organisations in which the tools and services have to be integrated.

This scheme could be based on a two-level assessment: (i) one level where a developer would be able to self-certify (e.g. by assessing an app through the criteria covered by a code of conduct) and (ii) another level where a national/regional entity would review the self-certification and the compliance of the product/service, providing certification (in order to avoid "re-certification" of the medical devices on the market, with a costly impact at a short-term for the producers, the elements covered by the certification would be the ones not covered by MDR and its notified bodies). Since it will merge into HTA national processes, the EU could encourage set up public-private partnerships to support certification processes according to the most suitable model (federated model including independent bodies with distributed roles or centralised model with governmental bodies and guidelines).

6.1.2 Define the scope of telehealth/mHealth products and services to be reimbursed

Although the Directive 2011/24/EU as currently shaped could allow for the reimbursement of some services such as telemedicine, more recent eHealth services might not be systematically included. For instance, as no legislation specifically addresses the mobile health environment and reimbursement laws are providing a narrow definition of mHealth, the definition of the scope should consider the evolution of the eHealth environments, becoming much broader as technology advances, especially mHealth. The aim is to ensure a better patient access to digital solutions which can clearly be considered for reimbursement in all countries, with an appropriate pathway to market access. Including such products/services by cooperating with Member States would provide benefits on patient outcomes by relying on their added value on quality, continuity of care, and overall efficiency of the healthcare system.

Option 1 Include eHealth products and services in the scope of revision of the Directive 2011/24/EU through European Health Data Space. According to the understanding of the Directive 2011/24/EU, services should be provided and reimbursed according to the same conditions, criteria of eligibility and regulatory and administrative formalities, whether set at a local, regional or national level, as it would impose in the provider territory. The clarification of the Directive 2011/24/EU will highlight how it applies also to telehealth and mobile health services, in order to extend the scope of services that can be reimbursed, by including eHealth products and services beyond telemedicine. The extension of the scope will encompass all the services which are currently not covered by the Directive, referring to: health data management such as personal health data spaces, non-medical digital health apps and some telemonitoring

products/services could be included in the national baskets for reimbursement but do not fall under the scope of the Directive.

This will support the decision of the MSs for reimbursement of the products/services as a healthcare or medicine, provided that the conditions for access remain the same as for normal healthcare. Considering digital health services specificities, the Member State of treatment would be considered, as per the Directive 2011/24/EU, the Member State where the healthcare provider is established.

Option 2 Support innovative pathways for digital health. An appropriate model should be supported at EU level to ensure that Member States establish early access pathways and value frameworks that are specific to innovative solutions (including telehealth, mobile health). To do so, one should experiment the design of EU-level digital healthcare pathways as part of the existing healthcare pathways in healthcare systems, by keeping a small scope at first and focus on one example (e.g. radiology or skin cancer). This should involve stakeholders such as healthcare professionals, insurers and regulators.

Such pathways would be fitted to the dynamic model and lifecycles of digital solutions, offering a fair model for SMEs to access the digital healthcare market. The definition of the components of such a model will be based on an alignment on the type of requirements and the evidence needed to support service providers when publishing their tools in multiple countries. As under options 1 and 3, this relies on voluntary mutual recognition principles between Member States, including in terms of reimbursement.

Given the importance to support digital health manufacturers in their effort to generate evidence and facilitate market access, the focus will be on the value of the outcomes. The national reimbursement practices are linked to positive outcomes on the users' health, with high value recognition for RWE, and such pathways will rely on effectiveness, clinical benefits and cost saving aspects, in a perspective to find game-changing practical use and scale up of the services.

Option 3 Replicate a current national model to the other Member States. In addition to option 2, the EU could use existing innovative access pathways among Member States (mHealth in Belgium, DiGA in Germany, Article 51 in France) as a baseline for replication in other Member States, with the objective to reduce country-specific requirements, which imply customised approaches for the products/services providers. The example could be the DiGA in Germany and the German law on digital health, setting-up a fast track certification and reimbursement scheme for mHealth apps. This could be set up through guidelines to encourage all Member States and rely on the national bodies dealing with HTA, digital health or other bodies at national level.

6.1.3 Facilitate the use of digital products/services and the access to patients' data

The objective is to ensure an access in electronic format and a compulsory transmission of patients' digital health records to the patient EHR when a digital health service is provided. Interoperability rules and exchanges of datasets will play a crucial role in this setting, where right incentives can foster the cross-border use. The national digital health bodies or other bodies would enforce rules suited for digital health beyond the rights set out in the GDPR.

It should also be established and enhanced the access to health data by healthcare professionals, by giving access rights to health data by healthcare professionals in electronic interoperable format, including of health data generated by patients abroad.

To do so, interoperability criteria for such electronic interoperable format would be included in the labelling and scheme established under options 1 and 3 of Need 1, to incentivise the exchange of information between healthcare providers of digital health services and products,

ensuring interoperability with the electronic health records and allowing patient access to their health data generated in the MST. One could envision a service of eHDSI allowing individuals to access, through their MSA (Member State of Affiliation) patient portal, health data generated in the MST, i.e. data flow is reversed. Furthermore, knowing about data generated in MST (Member State of Treatment) is also relevant for the health professional/system in MSA (could be another use case).

Such scheme would be established to incentivise the exchange of information between healthcare providers of digital health services and products (it should cover the entire ecosystem, from mHealth, telehealth, ehealth records, patient portals, my personal health data spaces ensuring interoperability with the electronic health records. It would cover for m-health services, requiring providers to share/store the data on the patients' EHR and supporting the sharing of patient's data with healthcare providers. Indeed, the access should be granted to health professionals in a patient-centred way, rather than through organisation to organisation or doctor-to-doctor interoperability models, since new European Health Data Space will have this human-centric nature

This would be implemented in cooperation with the bodies responsible for interoperability in the area of health, also building on the work performed by eHN and JAs, such as InteropEHRate and X-eHealth. The bodies dealing with digital health or other bodies/private entities recognised by the bodies dealing with digital health at national level would also cover interoperability between tele-health/m-health solutions, other digital health services and products, and electronic health records, as well as other quality elements as defined under option 1 of Need 1. Therefore, such bodies would provide a label to the manufacturers of digital health services and products and contribute to an overall quality label for telehealth, mHealth solutions and digital health services, supporting the Member States in their reimbursement decisions. A leadership from the eHealth Network on interoperability criteria could rely on the maturity of OpenEHR, HL7 FHIR standards and security standards.

Option 2 Extend the scope of services of the eHDSI on identification and interoperability to support data exchanges. As an important intermediary between Member States on security and interoperability issues, such extension of the services provided to the eHDSI/MyHealth@EU will allow the health data generated in the country of treatment to be sent to the country of affiliation. This would imply to ensure the users can identify themselves in eHDSI, vis-à-vis the other identification mechanisms in use for other health data portals and personal health data spaces and that the data is sharable across the different platforms.

Currently, the MS have different solutions in place to give patients access to their data, among which portals and personal health data spaces are the most common. As an example, MyData Operators is an organisation that could help bringing a citizen-centric design forward.

Supporting this action, the eHDSI would also provide implementation guides for APIs to help generate efficient interoperable data flows between national or pan-European digital health infrastructures and support the scale up of effective cross-border exchanges.

Furthermore, it could have a crucial role in defining the principles of a unique pan-European identification system relying on encoding keys, which should enable a secure European patient and healthcare provider identification, along with the identification of their relation. Such action is intended to foster cross-border exchanges and mutual recognition even with different national schemes and should rely on a mutual recognition across borders of existing identity schemes.

Option 3 Support ex-ante funding conditionalities to interoperability. An interoperability premium from national or EU funds could be introduced, provided to the services that would

ensure the cross-border interoperability of data. This ex-ante conditionality for EU funds (ERDF, RRF, etc.) will allow to finance digital health only if it complies with specific standards and specifications ensuring interoperability between electronic health records. This obligation should also be recommended to national procurers. This premium will guide investment and improvement towards cross-border telehealth mHealth and digital health infrastructure, avoiding local customisation issues.

Option 4 Define minimum datasets and standards to include in national procurements.

The Commission could either support or require the inclusion of precise standards and specifications in national procurements. Indeed, procurements, whether national, regional or otherwise, determine the design of IT solutions in health. In order to further develop the European EHR Exchange Format (EHRxF), such standard could be included to cover data specifications from digital health devices and services. A framework of relevant standards could be defined to ensure data interoperability aiming at technical and semantic interoperability standards. Such action could also be led on datasets, relying on the work already carried out (e.g. epSOS project and International Patient Summary) to build a comprehensive overview of compulsory datasets to be shared cross-border.

Besides, beyond the rights set out in GDPR, it should be ensured by legislation that access in electronic format and transmission of patients' digital health records is compulsory in all the cases where a digital health service is provided. For instance, when a patient benefits from telemedicine, the doctor would be able to access the patients' electronic health record; if the patient is tele-monitored/uses m-health applications/devices by a foreign healthcare professional, the information would be transmitted to the healthcare professional and to the EHR of the patient. The national digital health bodies or other bodies would enforce these rules.

Option 5 Support the inclusion of digital literacy and skills in HPs curricula. The EU could require Member States to adapt medical curricula with a baseline approach including horizontal topics on digital health (e.g. limitations of technology, digital communication with patients, understanding of telemedicine, smart devices, AI and big data awareness) for the undergraduates and (ii) specific classes with strong digital skills framed according to their medical specialty (e.g. cybersecurity, data protection). Such action is intended to support digital literacy, digital skills, knowledge of compliance regulation surrounding the use of health data along with fostering trust and acceptability through the HP-patient relationship. Besides, the EU should clearly identify the financing source of this training, with the intention to release the burden on the industry stakeholders.

To this end, the EU could also settle an EU-level mutual digital skills recognition for healthcare professionals, harmonising the qualifications among the Member States through a new accreditation, which could be a way to build a cross-border trust relationship. Such action would be performed by settling different levels of qualifications to match each Member State maturity in the field of digital healthcare, however it should be carefully assessed in a way to avoid creating an additional obstacle. Furthermore, the EU could be responsible for centralising the best practices regarding digital health practices. For instance, raising awareness on key roles for health adoption such as digital leaders in healthcare structures, who bear responsibility to introduce the technology to other healthcare professionals.

6.1.4 Ensure transparency of digital health services and products provided cross-borders

The aim is to raise awareness among users, both professionals and patients, to counteract the global lack of understanding around the processing, sharing and relevance of data generated

through eHealth, especially mobile applications. eHealth adoption, especially mHealth, will only be ensured by garnering the trust of healthcare professionals, thus their patients.

Option 1 Require a list of recognised, reliable digital health products and services. Member States should be required to provide a list of recognised, reliable digital health products and services, in collaboration with HTA bodies, notified bodies and national bodies responsible for digital health interoperability. This list should be made available through an API to facilitate visibility on the digital services and possibly their reimbursement, thus reimbursement bodies could be included. Such function could be included in the tasks of national contact points for the Directive 2011/24/EU, along with keeping it continuously up to date. An active public communication should be led on this impartial list of eHealth start-ups and companies to support healthcare providers in the adoption of eHealth tools. Furthermore, to this end, the EU could create a repository combining national repositories on digital health solutions that have proven to be cost-effective and medically beneficial.

Option 2 Involve healthcare professionals in building a transparent communication on the use of digital health. The involvement of HP in this communication could be led through funding their representatives and their organisations on specific actions intended to overcome trust issues on cross-border digital healthcare and health data sharing obstacles. Such action should be performed through non-legislative measures (e.g. communication campaigns in hospitals; trainings, etc.). Such communication would aim at fostering citizen's digital literacy, ensuring adoption of telehealth and mHealth products/services, as well as providing sufficient information to the patient on the secondary use of the data. It could also focus on the various benefits of sharing health data, which would likely make people more inclined to share their data, as well as on the individual and collective value of sharing their data, raising awareness on benefits and health added value both for their own good and the common good. This communication could be made through an official European website but also by the healthcare professionals themselves using the trainings provided. There would be a real benefit for this communication around the processing, sharing and relevance of data generated through digital health to be endorsed by a doctor as a trusted actor in healthcare.

Foster more consistency in the national GDPR implementations in the area of health data processing. The control of patients over their data could be emphasised in mHealth regulation, building upon the GDPR: the data-subject could decide on the storage (e.g. EHR, device) and the sharing of data, eliminating any obligation for the patient to store his mHealth data on the servers of the manufacturer.

Support the establishment of an appropriate consent model. Since the need goes beyond GDPR consent in medical research, the EU should find an appropriate consent model which encompasses "re-consenting" cases, including an appropriate granularity with a balance between the right level of access and control over their data by the patients and the possibility to unlock it for the public good. It should be considered a first step towards initiating European ethical, GDPR-compliant, quality-controlled data spaces, possibly based on AI algorithms. The European Commission could start working on specific use cases such as rare or chronic diseases to build and manage a suitable model, since they represent a smaller number of patients willing to share data and requiring a strong cooperation.

6.1.5 Ensure an appropriate liability framing for digital health

The objective is to identify a clear guidance on liability, suited for digital health products/services, including those based on AI, through an adequate detection of barriers under existing procedures (e.g. 2015/1535). Such action is intended to ensure mutual recognition of national rules

providing the same level of protection, with common rules whose compliance will ensure that the less additional rule possible will be imposed to digital health products/services.

Establish a framework for liability when using digital health products and services. A framework would be issued at EU level, indicating any specificities of such products and services in healthcare, the role of physicians, the needs of patients, the best interests of patients in using and be subject to digital health including AI. The framework where the tools are being used considering the context of use (e.g. when the patient uses or looks for a service on his own, or when a healthcare provider prescribes the use of an application). The framework will describe the conditions and the rules that apply (e.g. pre-existing relationship with the patient, follow-up, monitoring, post-operation consultation, etc.), highlighting the responsibility of physicians or providers on their use, including prescription of non-medical applications or non-certified services. Furthermore, guidelines on data protection and ethical requirements could promote the adoption of specific digital services clarifying their liability (e.g. IMApps for secure messaging between clinicians).

Ensure mutual recognition of national rules providing the same level of protection. A mutual recognition issued through binding legislation would support similar rules whose compliance ensure that no additional rule will be imposed to digital health products / services, especially those under MDR (e.g. Data protection, Cybersecurity, Interoperability, Safety). Such action would be carried out by creating a model or rules that would be incorporated in other legislatives frameworks (such as the products liability directive) that would be fit for healthcare and safeguard the best interests of patient that are distinct from ordinary consumers of other products and services.

Develop non-binding guidance supporting the Product Liability Directive. Non-binding guidance could be issued to avoid introducing legislative changes but rather clarify some issues under the Directive. Even though the Directive continues to be fit for purpose, the technology continues to develop at high speed, as a result, legal and regulatory frameworks might struggle to keep the pace. Further guidance will for instance enlighten whether the producer of a product can be held liable where that product is defective, or producer of a product will typically be the same entity as the one that is responsible for the safety of the product under other legislation, also clarifying the duty on distributors and suppliers to help consumers identify the producer of a product. A clear adherence will also be shown with the Commission's Better regulation guidelines to provide a simple, clear, stable and predictable regulatory regime.

6.2 Artificial intelligence in health

As presented in previous sections, AI systems in general have particular characteristics that create different challenges for ensuing their proper application in different domains. This statement gains more importance when we talk about AI systems used in the healthcare domain, where they can have a strong impact on patients' health and life. For this reason, specific EU and national legislations should take into consideration the characteristics of AI-based systems and the specificities and legal provisions related to the area where they are going to be used and that protect fundamental rights, attribute liability and meet the necessary conditions to claim compensation (EU Commission, 2020).

Despite the promises about AI systems in health, there is a slow and limited uptake of digital health products and services which integrate AI. The main cases from a regulatory and governance point of view could be grouped in three main areas:

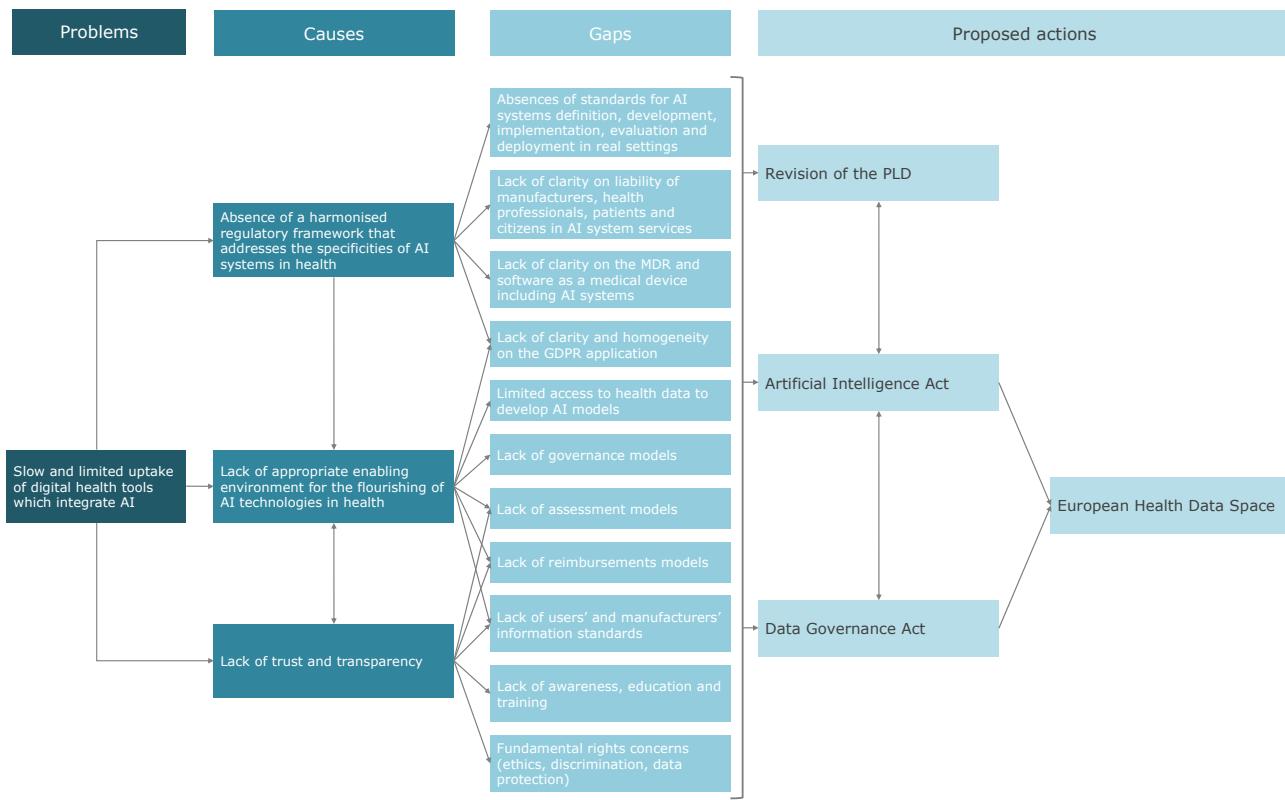
- Absence of a harmonised regulatory framework that addresses the specificities of AI systems in health.

- Lack of appropriate enabling environment for the flourishing of AI.
- Lack of trust and transparency.

It is important to point out that these causes were identified at both Member States and EU level. These causes identified during the study can be explained by the existence of several interrelated gaps:

- Absences of standards for AI systems definition, development, implementation, evaluation and deployment in real settings.
- Lack of clarity on liability of manufacturers, health professionals, patients and citizens in AI system services.
- Lack of clarity on the MDR and software as a medical device including AI systems.
- Lack of clarity and homogeneity on the GDPR application.
- Limited access to health data to develop AI models.
- Lack of governance models.
- Lack of assessment models.
- Lack of reimbursements models.
- Lack of users' and manufacturers' information standards.
- Lack of awareness, education and training.
- Fundamental rights concerns (ethics, discrimination, data protection).

As discussed in section 3.2.4, the current proposed EU initiatives, Artificial Intelligence Act and the Data Governance Act (together with the forthcoming European Health Data Space), are currently establishing the ground to address most of these gaps, showing the potential added value of the EU intervention to facilitate access to safe and high-quality cross-border healthcare in the Union and to ensure patient mobility guaranteeing the free movement of goods and services and the consistency with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality. The following figure sketches the main problem, causes, gaps and proposed actions. Developing data governance systems with respect to AI will be crucial to the development of this technology.

Figure 18. AI system in health: problem, causes, gaps and proposed actions

Source: Authors' elaboration

Experts consulted for the stakeholders' consultation also consider that maybe it is not necessarily a matter of creating something new but a matter of ensuring that the AI framework includes instances to increase digital health literacy and involvement of the different actors in the design and development process of AI systems. In this sense, new legislations, regulations and standards need to be developed in alignment with current regulatory frameworks so the adoption of AI-based system in the healthcare sector can be smooth, quick and responsible (Rowley et al, 2019), reducing the minimum requested level of formal legislation.

Some considerations that can be useful to do this are (Gruson et al, 2019): (a) implement patient information and consent prior to the use of any AI technology in the course of their care; (b) allow the possibility to request a second opinion from a human medical expert (for both patients and healthcare professionals); (c) identify levels of sensitivity of healthcare data in order to provide regulations according to these levels; and (d) adapt and update healthcare profession principles taking into consideration AI systems. Systems that require frequent software updates, or which rely on machine learning, can produce new risks that were not present in the initial approved system deployed.

This situation is not adequately addressed in the existing legislations which predominantly focuses on the risks present at the time of placing the system on the market (EU Commission, 2020). In this regard, the Parliament suggested the Commission to revise the list of high-risk applications every six months, because the speed of change is so fast, but this might create problems in terms of business and investment because the cost of a product might change if after six months you do not know if your software will be classified as high risk or not.

The following sections presents recommendations based on the current needs and gaps identified with the study literature analysis and including the feedback obtained through the stakeholders' consultation.

As it has been described in chapter 3, AI in health spans across several areas (see Figure 3) involving different stakeholders from the intended purpose, end users' qualification and level of control till data collection, preparation, transformation and modelling till the evaluation and deployment in real settings (see Figure 5). During all these phases, data governance mechanism, including data protection, security and quality, plays a critical role. Despite the contribution and risks of AI in health, there is a lack of regulatory framework both at Member States level and at EU level. Moreover, the existing frameworks (see section 3.2.1) show some gaps that might hamper the development of AI in health. The proposed DGA (and the forthcoming EHDS) and AIA are establishing the grounds to cover these gaps.

AI systems legal definitions should be well-defined by European regulations in order to facilitate the creation of legal principles that lead to levels of responsibility and consequences. DGA and AIA provide the horizontal frameworks. The EHDS could further embed this into the health domain (e.g. Box 24). The AIA also defines key terms (Art. 3) that could be further specified by the EHDS establishing clear data governance tools. The AIA establishes requirements for high-risk AI systems. The operationalisation of these requirements notably in the view of the consideration of sectorial applications is done through standards, based on the principles of Regulation 1025/2012. Moreover, guidance can be produced by the Commission. It is key that for healthcare AI systems, EDHS and MDR governance bodies are appropriately involved in the elaboration of standards and guidance under the AIA, notably with regard to key healthcare-related aspects: interpretation of definitions, information to patients, monitoring of health AI systems, transparency and explainability. It is expected that the EHDS will facilitate the creation of data permit authorities. It is important that the EHDS provide tools to ensure the appropriate involvement of those authorities in AIA standardisation/guidance.

AI systems information. The AIA risk-based approach could be complemented with different types of applications (see Figure 4) based on the level of qualification of the end-users, the type of outcomes and the level of human control. All these elements will guide the information accompanying the AI system, including the type of approval, certification, authorisation as well as the safety and security measures (e.g. warnings and labels). This could also be applied not just to the AI system but also to the data used to develop the system. For example, **more information for the patient** emphasizing the risks and benefits of using AI-based systems in their care. AI-based systems need to provide information to patients, as the medicines with the information of adverse effects or risks.

Implement mechanisms to clearly establish the relationship between the responsibilities of the AI system, the healthcare professional and the patients, especially when AI system entails the provision of a service. Scientific communities, professionals' associations, patient representatives together with legal experts and AI systems developers and manufacturers shall engage with the regulators and health authorities to better clarify these responsibilities. It is very important to transmit to the physicians the level of reliability of the tests and how they are done to allow interpreting results correctly in the context of the clinical environment with the rest of the variables. This allows doctors to derive the value from what artificial intelligence can contribute, as another instrument. For this, it is necessary to differentiate a malfunction of the system from a wrong decision. If it has a bad function due to bad design, responsibility has to be more focused on the manufacturers. Another thing is if the result is not as expected based on decision making. In this case, a probabilistic relationship would have to be analysed. Medical error implies a subjective component that could be interpreted as not voluntary on the part of the professional. There is a need to clarify the type of warnings or labels in all the phases of the AI systems, from the raw data to the utilisation of AI in real settings.

There is a need to provide clear legal framework at EU level on how the **obligations of the manufacturer** should be if there is a learned intermediary (e.g., healthcare professionals). A common mechanism across Europe will reduce the legal uncertainty of having different courts and legal regimes between MS. This legal mechanism may include foreseeability as a determining factor defining manufacturers' obligations and responsibilities. In this regard, there is a need to set-up appropriate processes and protocols for healthcare professionals/providers as to how evolution of the AI system is monitored and controlled. There will be strong presumptions for negligence if processes and protocols are not in place. Negligence per se would be also applicable in this case, i.e., non-compliance with regulatory frameworks would indicate negligence. It would be possible to take non-compliance into account in the PLD – it could, for example, lead to an easing of the burden of proof.

Developers, health professionals and health authorities will also need more information, including guidance to navigate all the AI system phases (Rowley et al, 2019). **Evaluation guidelines and standards for AI algorithms in health**, including testing and certification mechanisms, should be available to carry out pre-development and post-development review of the output, the algorithm applied, and the progress and post-implementation reports (Zuiderveen & Borgesius, 2020; Esmaeilzadeh, 2020). The EHDS shall define these standards and guidelines enabling auditing and evaluation of safety, quality, transparency, and ethical factors through well-established and regular monitoring processes to evaluate the AI-based systems in each new context before using them in patient's care (Carter et al, 2020). Such standards could be developed by the data permit/access authorities in the area of health, alone or in cooperation with the authorities responsible for AIA. AI systems require careful development, testing and evaluation in each new context before use in patient care (Diebolt et al., 2018). EHDS shall establish a common European normative standard and evaluation methodologies for the design, development, deployment and use of AI in healthcare. This includes the relationship with other bodies (e.g., HTA agencies) and regulations (e.g. MDR, GDPR).

Professional bodies will need to reinforce their engagement with regulatory agencies and standardisation organisations on legal and technical issues, and develop common standards for evaluating, validation, and testing AI systems. It is expected that the EHDS will facilitate the creation of data permit authorities. It is important to clarify also how these authorities will engage with current bodies such as HTA agencies, notified bodies under MDR or authorities of AIA. Moreover, there is a need to clarify the role of the private sector (e.g. Medtech and Pharma) and how they will interact with the proposed data authorities during all the AI system phases.

Data governance. AI algorithms have to be trained with a large amount of data that sometimes is not available across all Member States. Availability of high-quality dataset is essential to guarantee strong AI models and trustworthy outcomes, especially for cross-border care provision. An **EU common framework for the exchange of data across borders**,²⁴¹ through strong governance models, is needed to foster AI impact and enhance AI benefits in healthcare (ESR, 2020). GDPR regulations could be enhanced taking into consideration anti-discrimination law concepts as a way to unlock the algorithms and provide interpretability and transparency while ensuring fairness. AIA and the forthcoming EHDS should clarify the data governance principles in health. While considering the highest standards of data protection, security and quality, both AIA and the forthcoming EHDS should have to balance these standards with realism considering the feasibility of the options and also the appropriate market incentives, avoiding an excessive burden in the public authorities and the private sector. Having a single entrance to

²⁴¹ Lessons learned from current initiatives such as EOSC Life, 1 Million Genomes, EHDEN... could be extended and applied to AI.

data might require capacity issues if there is a high demand. In addition, having a single entrance might hamper access to specific data that has not been processed by the data authority, but it is available within a specific healthcare services provider. How data authorities will deal with the data within each health systems remains uncertain specially in Member States with lower levels of digitalisations and decentralised health systems. This might also happen in the case of data quality criteria and the context of Real World Data. There is a need to define what data quality means, from the intended purpose of the AI system (e.g. using NLP to codify clinical notes) and the raw data to the data preparation and data transformation and modelling. Consensus among all the stakeholders is needed to establish the role of data quality and the evaluation and replicability of the outcomes of the AI systems.

Find a balance between access to data and their protection, support access to health data for training of algorithms, and the potential interference with the physician–patient relationship. There is **still a disparity between accepting information from one country to another** avoiding cross-border accessibility and, consequently, making difficult cooperation between EU Member States. Consistent and robust regulations and polices related to the access, harmonisation, interoperability, use, sharing and storage of healthcare data at EU level, are principal in order to remove the barriers towards cross-border healthcare provision and patient mobility. Guidance for Member States to adopt legislations that harmonises the legal base to be used for the **processing of health data for scientific research and innovation**. Sharing data across Member States is central to advance AI research and implementation. AI in healthcare will gain considerably from cross-border collaboration in the processing of personal health data.

EHDS envisages the creation of data permit authorities in charge of regulate data access by third parties, for example for secondary use, providing or authorizing the access to data when some conditions are met. This could be useful for data sharing for research purposes or for training and testing AI algorithms with wide sets of healthcare data. Data permit authorities could support access to data for training of AI algorithms and could also support regulatory bodies (notified bodies for medical devices, medicine agencies) with control datasets, supporting them in the evaluation of different AI algorithms. These authorities should follow the same standards and guidelines to coordinate their efforts and avoid additional transaction costs. The example of the eHN (see chapter 5) shows that voluntary bases won't facilitate the Digital Single Market.

Involvement of all related stakeholders (e.g., primary stakeholders - healthcare authorities, healthcare providers/hospitals, chief information officers, or chief data officers, commercial companies providing AI based products and services, the local regulatory authorities, and the end-user / Patient) is an important aspect to consider during the process, from design to deployment and use in healthcare settings (Baig et al., 2020). Healthcare professionals interviewed pointed out also the importance of including the stakeholders, and specifically the patients, in order to know their expectations and how they perceive the use of these systems and with the objective of helping them. Making any kind of systems for helping the patients without count with them, it would be a real antithesis.

Transparency and explainability of AI are complex and emerging concepts. If these concepts are used in guidelines or legislation, they should be developed in **close collaboration** with data scientists to ensure that requirements can be executed and have real value (EIT Health Consultative Group, 2020). The relationship between AI-based systems manufacturers and health professionals has to go hand in hand, from the objectives of the AI system so that they know what sort of expectations there are, understand and trust in them by knowing its performance, accuracy, and outcomes.

Sustaining trust and trustworthiness is a key goal of governance, which is necessary to promote collaboration among all stakeholders and to ensure the responsible development and implementation of AI in healthcare (Ho et al, 2019). When trust is ensured, patients and healthcare professionals' willingness to use and invest in AI increase, and this allows to have AI in healthcare playing an important role.

Promote responsible algorithms “by design”, that integrate elements allowing the traceability and the explicability of the results as well as controls ensuring the absence of potential negative effects of the algorithms (Diebolt et al, 2018). The more open the system, the more security the professional will have. In the end it is the concept of collective knowledge, it is one of the things that helps the most and is closest to the results. The obligation of the manufacturer to provide information to the injured party is part of the transparency obligation. When you have a regime that enforces transparency, then the party can easily show what were the defects, so that should be embedded in the system through the transparency requirement.

Regulations and policies have to consider AI ability to adapt to different users and contexts. Like the car industry, AI-based systems used in healthcare should be defined as categories and autonomy levels (e.g., Figure 4). Since law may not cover all aspects in all cases and all conditions, we should have a common and well-established ethic framework that is accepted by society

6.3 Governing the use of health data

6.3.1 European Health Data Space

The creation of a European Health Data Space (EHDS) was set as one of the priorities of the Von der Leyen Commission in the area of healthcare digitalisation and was listed in the Commission Work Programme 2021 and the European Strategy for Data adopted in February 2020. The objective of the European Health Data Space is to promote better exchange and access to different types of health data (electronic health records, genomics data, data from patient registries etc.), not only to support healthcare delivery (primary use of data) but also for health research, innovation, health policy making and regulatory decision purposes (secondary use of data). Moreover, the availability of high quality data facilitates operator's compliance with the new AI regulation proposed by the Commission on 21 April. The EHDS should ensure the protection of citizens' data and facilitate the portability of health data in line with GDPR. It is important to note again that the GDPR allows derogation for Member States to maintain/introduce further requirements regarding health data.

The Commission, in collaboration with the Member States, is already engaged in the preparatory work and development of the EHDS, via a “Joint Action Towards the European Health Data Space” and various consultation activities. The European Health Data Space will be built on three main pillars:

1. a strong system of data governance and rules for data exchange
2. data quality
3. strong infrastructure and interoperability

Regarding the sharing of health data for healthcare purposes (primary use), some conditions should be respected, including:

- Healthcare providers need to have digital systems in place to exchange data securely with other health professionals and digital health devices.

- Healthcare providers need to comply with the applicable provisions of the GDPR, the requirement to rely on a legal basis in order to be able to lawfully exchange health data cross borders.
- Data need to be in the same format and correspond to a common data quality, cybersecurity and other interoperability standards on which healthcare professionals can rely.
- Relevant mechanisms may also be implemented to support the uptake of these standards (such as labelling, certification, authorisation schemes and codes of conduct).
- Cooperation of national digital health bodies is needed for the development of interoperable standards and specifications.

6.3.2 Policy options for primary use

To address the issues identified with the exchange of data for primary use and to ensure a common framework and governance for healthcare data quality assurance and interoperability, several policy options revolve around the setup of digital health bodies at EU and/or national level, that could be entrusted with different tasks (e.g. interoperability, tele-health, m-health, security of data storage etc) with different intensities of actions (e.g. from labelling to certification). **National digital health authorities could be entrusted with tasks related to cross-border digital health**, such as technical specifications for data quality and interoperability, security of data infrastructures, labelling/certification/authorisation schemes for healthcare providers and for digital health products and services (see chapter 2). These national digital health bodies should cooperate at EU level and could gather in a **new mandatory advisory committee/expert group** in charge of making guidelines on technical specifications for interoperability, and of steering the development of MyHealth@EU. A governance framework for primary use of health data could be established at EU level, with the **Commission adopting guidelines on minimum datasets and standards** to be used when sharing health data between healthcare providers. The **minimum datasets to be exchanged cross-border for healthcare purposes** could be determined by non-binding guidelines or by binding legislation.

To lower technical barriers hindering health data use and re-use and portability, the use of the **European Health Record Exchange Format** and of **specific standards and specifications** could be made mandatory by the Commission for specific health data exchanges. A scheme for labelling, certification or authorisation could be introduced for healthcare providers in relation to their compliance with health specific standards and specifications for interoperability (see chapter 2).

To make sure that **interoperable procedures and standards** for exchange of data are applied in Member States, these could constitute an **ex-ante conditionality** to EU support funds (e.g. ERDF, RRF). In addition, the respect of certain standards and specifications for interoperability could be encouraged or made mandatory in procurements. Alternatively, an interoperability premium could be provided from national or EU funds for services that ensure the cross-border interoperability of data.

Other policy options to improve the exchange of health data for primary use concern the potential **evolution of the IT infrastructure related to the eHealth Network (eHDSI/MyHealth @ EU)**. The use of MyHealth@EU for the cross-border exchange of patients' data when traveling abroad could be expanded to **cover data exchanges between all Member States and could become mandatory**. An ad-hoc sub-group within the eHealth Network could provide support and capacity building to Member States lacking the technical capacity to set up and run the infrastructure. MyHealth@EU could continue to be used for the exchange of patient

summaries, ePrescriptions, images, laboratory results, discharge letters, and **could expand its services** (e.g. allowing patients and health professionals to directly access their health data and incorporate them into their EHR). Various options could be explored for the operational implementation of MyHealth@EU, including keeping the current delivery model (grants for Member States to set up the national contact point and IT core services done in DG SANTE, with CEF support), use an EU agency to manage the implementation of the infrastructure, set up a public-public partnership or a public-private partnership under the EHDS proposal, set up a non-for profit organization, or use an existing research infrastructure/body/structure (see chapter 5). Fostering the private sector to engage with MyHealth@EU could facilitate the acceleration of the Digital Single Market for digital health products and services (see chapter 2).

To facilitate the use and control of citizens over their health data, the national digital health bodies could enforce **rules to ensure citizens' access to and transmission of their own health data in an electronic format**. Pursuant to the **once only principle**, patients should be able to provide their health data once and make it available to other healthcare providers or professionals based on their consent/permission. MyHealth@EU could be transformed into the European e-Patient platform allowing third parties from the public and private sector to offer products and services with the authorisation from the users.

6.3.3 Policy options for secondary use

With regard to the exchange of health data for research and innovation, policy-making and regulatory decision (secondary use), the Data Governance Act²⁴² proposes rules on access and sharing of data across sectors, on access to data held by public bodies, on data intermediary services for B2B and B2C sharing of data, and rules on sharing of data by individuals and companies through a trusted third party for wider good purposes (e.g. research) and based on their consent. **The Data Governance Act allows for the possibility for additional sectoral legislation** to set up and further specify the role of national bodies taking decisions on access to data by third parties. The upcoming Regulation for a EHDS would provide the legal basis for additional provisions on data exchange in the health sector.

To establish a legal and governance framework on the access to and exchange of health data for secondary use, several policy options revolve around setting data authorisation bodies at national and/or EU level, entrusted with different tasks on data availability and access, training of AI systems, data altruism etc, with different intensities of actions (from labelling to certification), as well as national and EU digital infrastructures for secondary use of health data.

On top of the creation of a national single point of information foreseen in the Data Governance Act, Member States could be encouraged or required to have a **national data authorisation body** entrusted to handle requests for access to health data, where relevant to grant a licence/permit for access, and to provide the physical infrastructure to enable access to health data for secondary purposes, including for the training and testing of AI algorithms. To build trust in consenting the use of health data for secondary use, Member States could run an educational campaign to inform patients on how sharing their health data for secondary purposes could lead to progress in treatments and innovative medical breakthroughs.

At EU level, cooperation on secondary use of health data could be ensured by the eHealth Network with relevant representatives Member States on secondary use of health data, or by the creation of a network or an advisory group to the Commission gathering the national data authorisation bodies, to support the Commission on interoperability rules and infrastructure for

²⁴² Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). 2020/0340 (COD).

secondary use of health data, and for setting requirements for data altruism in the health sector. Alternatively, an EU body could be set up to coordinate the work of the data authorisation bodies, acting as a **European Data Authorisation body** that hosts and/or queries EU wide databases and registries established under EU law or bringing data from several Member States. For any of these options, the governance mechanisms at EU level for the secondary use of data could provide for a regular channel for mutual information with those established for the primary use of data. Lessons learned from the eHN could be applied into the new institutional design (see chapter 5).

Access of business data by the public sector (B2G) could be mandated by national/EU law or done by direct mandate. The transfer of data could be supported by the data authorisation bodies or done directly through agreements with data holders. **B2B access of data between private sector entities** could be done through the intermediary of data authorisation bodies if mandated by law, provided that the data subject consents. Both for B2G and B2B access to data, a fee could be introduced. The transfer of health data to stakeholders outside the-EU/EEA should be subject to compliance with data protection rules for international data transfers and to conclusion of specific agreements.

In order to lower technical barriers hindering data access and re-use, data quality and interoperability **specifications and standards** for stakeholders contributing and/or receiving health data for secondary use within the European Health Data Space could be established and incentivised by a labelling scheme or made mandatory with a certification or authorisation scheme. An **EU interoperable digital data infrastructure for secondary use of data** could be set up, connecting data authorisation bodies, public bodies (including national bodies and EU bodies such as EMA and ECDC) and other authorised relevant stakeholders, for queries and access to health data.

Various options could be considered for the **operational implementation of the infrastructure**, including providing the same delivery model for EHDS as the one for MyHealth@EU (grants for Member States to set up the national node and IT core services done in DG SANTE), use an EU agency or an existing health digital infrastructure, set up a public-public partnership or a public-private partnership under the EHDS, or use an association or a private entity to manage the infrastructure.

In terms of the **operational implementation of the EU Data Permit Authority**, several options could also be envisaged, including setting up a public-public partnership or a public-private partnership, use an EU agency (e.g. EMA, JRC), an existing/new ERIC (European Research Infrastructure Consortium), an association or a private entity.

6.4 Evaluation of Article 14 of Directive 2011/24/EU

The 2017 report on the State of Health in the EU²⁴³ concluded that only by fundamentally rethinking our healthcare systems we can ensure that they remain sustainable and fit-for-purpose. This means systems which aim to continue to promote health, prevent disease and provide patient-centred care that meets citizens' needs. Healthcare systems require reforms and innovative solutions to become more resilient, accessible and effective in providing quality care to European citizens.

Effectiveness. As of today, after almost 10 years of activities, the effectiveness of the eHealth Network action has been very limited and concentrated in enhancing the use of health data for primary purpose in the context of cross-border healthcare. More specifically, most of the

²⁴³ State of Health in the EU "Companion Report 2017", <https://ec.europa.eu/health/state>

activities focused on drafting guidelines for **ePrescriptions** and **patient summaries** and to support the development of the **MyHealth@EU infrastructure** to enable electronic cross-border health services. The MyHealth@EU platform has been implemented in 8 Member States²⁴⁴ and other 3 are supposed to join these exchanges by the end of 2021. Member States with decentralised healthcare systems and lower levels of digitalisation appeared to have a lower level of readiness to implement the developed tools. The platform currently supports two services (ePrescriptions and Patient Summaries), whose use has overcome the expected targets as set in the eHDSI Monitoring Framework (KPIs)²⁴⁵. However, the voluntary nature of the guidelines for implementing this platform and the fact that the infrastructure was voluntary, impacted on its take up and on the right of patients to ensure access and control over their data. In the future the platform should become mandatory to allow the patients to share their health data cross-borders and the types of data, standards and specifications should be established through delegated/implementing acts. The platform may be used to extend the amount of services provided and could constitute a starting point for the development of the EHDS. The very limited activities in the areas of patients access to their health data, telemedicine and secondary use of data resulted in a very low impact and therefore level of effectiveness in these areas. Part of the low results in patients access to their health data is linked to having Article 4.2 (f) and Article 5 (d) not strengthening the digital component. Such activities should be further developed, also in line with the recommendations related to digital health services (including electronic health records, m-health and tele-health), aiming at labelling and certification/authorisation. The provision of tele-health and m-health should be included in the normal provision of healthcare, without the need for a physical move of the patient.

Even if some of the activities of the eHealth Network were also aimed to support national interoperability, the impact of its decision making (voluntary guidelines) remained limited by their non-binding nature. At the same time, Member States set up digital health structures and in some cases they used the information, standards and specifications developed at EU level. A more systematic and compulsory setting up of standards and specification at EU level, as well as labelling and certification (also in line with the recommendations on digital health services and products) could increase significantly the effectiveness of the EU cooperation and contribute to the digital single market.

Following the outbreak of the COVID 19 pandemic in Europe, the eHealth Network provided support in developing the **contact tracing in the EU's fight against COVID-19** as well as supporting the development of interoperable **EU Digital COVID Certificate**. These activities are linked to public health instruments, interoperability of applications and free movement of people. Activities in the field of mHealth and telehealth were steered by a specific subgroup of the eHealth Network, but the follow up of the recommendations was limited after the end of this group. M-health activities increased during COVID-19 pandemic, with contact tracing app and EU digital COVID certificate. As mentioned above, in the future, such activities should be expanded also taking into account activities suggested under digital health services.

Support from the eHealth Network to Member States in developing effective methods for enabling the use of medical information for public health and research was not effective. Some documents on big data were produced, but they were not followed up by additional actions. At the EU level, some relevant activities in the area have been carried out by research projects funded by RTD and DG CONNECT. Since February 2021, the establishment of the TEHDAS Joint Action has relaunched EU intervention in the area and brought together the institutions dealing

²⁴⁴ End of 2020

²⁴⁵ <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=35210477>

with secondary use of health data. The Data Governance Act and the forthcoming European Health Data Space will play a crucial role.

Efficiency. While the eHealth network proved to be fairly effective and efficient in times of political convergence following the COVID 19 pandemic outbreak, previous initiatives presented some issues in terms of efficiency. While in the case of the EU Digital COVID certificate, the initiative was legally supported by a regulation²⁴⁶, in the case of the MyHealth@EU platform, no regulation on standardisation and harmonisation was proposed. This, combined with a voluntary cooperation framework that did not manage to secure sustained commitment by all Member States, might have hampered effectiveness.

As a result, so far only 8 Member States have implemented the MyHealth@EU platform (and other 3 are expected to join by the end of 2021). Different level of commitment by different countries is partially linked to different national priorities as well as different level of readiness. When Member States were enquired about the extent at which the eHealth Network support contributes to a more cost-efficient development of cross-border digital health resources, the vast majority did not have any strong position. As more Member States implement the developed tools and platforms, the more efficient their development and maintenance will be. Currently, all Member States are expected to implement the MyHealth@EU platform by 2025. The EU definition/selection of interoperability standards and specifications and a more systematic national implementation could support a uniform approach to interoperability and reduce the costs for developers to provide digital services products and services within Member States and across borders. It would also reduce the costs of healthcare systems, as data could be shared between healthcare providers within countries and between countries, without the need to repeat the same tests several times.

The lack of data collected for certain cost categories (Man Days and national investments to implement developed tools) resulted in difficulties in assessing the costs incurred by the different stakeholders.

Relevance. Digital solutions for healthcare can increase the well-being of millions of citizens and radically change the way healthcare services are delivered to patients, if designed purposefully and implemented in a cost-effective way. Digitisation can support the continuity of care across borders, an important aspect for those who spend time abroad for business or leisure purposes. In terms of relevance, while some issues such as the development of eID, the MyHealth@EU platform and common guidelines for patients summary and ePrescriptions have been addressed, most of the initial needs remains relevant as barriers to interoperability remains. Nalin (2019) identified several barriers towards the actual adoption and implementation of data exchange initiatives, namely;

- Not all EU Member States are aligned with the JASeHN agreement (and the IDAS regulation)
- Different consent mechanisms exist among Member States
- Lack of standard EHR system in Member States.
- Different implementation of EU regulations among Member States²⁴⁷
- Different information workflows among National Infrastructure and healthcare organizations

²⁴⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130>

²⁴⁷ Regulation 2014/910/EU and Regulation 2016/679/EU

- Lack of harmonization in rules, processes, and safeguards
- National Contact Point for eHealth deployments in Member States are still in early stages and they are not compulsory
- Lack of the budget to address security aspects by healthcare organisations

The technological innovation highlighted in chapter 4 and reflected in the EU policy evolution discussed in section 5.3.5 suggest that **the digitalisation of healthcare as actually increased the need for greater interoperability and data flow, both for HER and also in the context of telehealth and mHealth**. This is particularly true in the case of secondary use of data, which has only been recently started to be tackled by the TEHDAS Joint Action. Looking ahead, the setting up of the European Health Data Space for both primary and secondary use represents an important milestone to enable greater use of medical information for public health and research, but also highlights the need for greater coordination at the EU level to ensure coherent effort.

Coherence. In terms of coherence, the eHealth Network has been, at least on its intentions reflected in the MWPs, coherent with the policy evolution that took place over the last few years, especially with the development of the Digital Single Market Strategy, and more specifically the EU e-Government Action Plan 2016-2020, although some areas were not properly followed up upon, such as telehealth and eHealth. Member States national policies were not always aligned with eHealth Network activities and that may partially explain the current low pick up rates of some of the tools developed (i.e. MyHealth@EU platform) and some differentiation of interoperability standards and specifications. The recent setting up of the **THEDAS JA focusing on use and re-use of Health data and involving new actors in the process, has complemented** an area overlooked by eHealth Network but where Member States have carried out many activities. As article 14 of the Directive requests the eHealth Network to develop guidelines on effective methods for enabling the use of medical information for public health and research. The current situation calls for expanding the cross-border services offered to include secondary use of health data to develop the planned European Health Data Space.

EU added Value. In terms of EU added value, the result is mixed. While the pool of people potentially benefitting from cross-border healthcare is high, the patients taking advantage of this possibility is currently low although increasing. Also, there is a lot of potential for supporting people access to their health data, portability and re-use of this data, as well as provision of digital health services and products, including electronic health records, telehealth and m-health within and between different Member States. This can be seen both because of the lack of interoperability still present within and across the different national systems, but also as a relatively low demand for cross-border healthcare compared to national demand. While the EU contributed to the development of common standards for ePrescriptions, Patients Summary and eID, the pick-up rate and the resulting interoperability remains low. Furthermore, while the political support of most Member States for greater interoperability have been fairly low throughout the life of the Network, the outbreak of the COVID 19 pandemic not only highlighted the greater effectiveness of the network when there is political convergence, but it also highlighted **EU added value of having an integrated system that can enable effectively the use of medical information for free movement, public health and research.**

Based on the analysis carried out, we propose the following recommendations:

- Article 4.2 (f) and Article 5 (d) should be revised to strengthen digital access to data, portability and re-use of data, both at national and EU level. This will support free movement and will incentivise the application of rules to provide digital access to a copy of the medical record/s for patients affiliated to their healthcare system seeking cross-

border healthcare in another Member States as well as copy of the medical record/s of received treatment/s for patients affiliated to a different healthcare system that used cross-border healthcare in another Member States. It should strengthen the right of access to data and portability of data between healthcare providers within Member States. This could also flourish the number of potential interoperable applications available and therefore the Digital Single Market.

- Creating ad-hoc regulation to support the network initiatives, (i.e. the MyHealth@EU platform) should be enhanced and all the Member States should participate in this platform, allowing the patients to share their health data cross borders. The types of data, standards and specifications for sharing them should be enshrined in delegated and implementing acts. Patients could be given access to MyHealth@EU platform to increase their direct access to personal health data in a cross-border environment extending the number of services available on the platform. The services provided on the developed MyHealth@EU could be expanded to accommodate additional services in the space of tele-medicine, tele-health, tele-monitoring. However, digital health services (tele-health and m-health) could be provided between healthcare providers between Member States, not only as part of the provision of healthcare (without necessarily entailing a physical move of the patient).
- Further actions are needed to facilitate the access of health data to patients, ensuring the control of citizens over their own personal health data and the use of data for medical diagnosis, public health, research and policy making. Patients can be the driving force. A potential solution could be making the MyHealth@EU platform available to patients and extending the number of services available on the platform. Further actions are needed to support implementing the GDPR provisions of data subjects' access to data and portability of this data, allowing to avoid unnecessary repeated tests, entailing important costs. Taking advantage of digital health authorities that exist in all Member States and had proved their cooperation, this cooperation should be taken one step further. Such authorities should have a clear role at national level to provide access and portability of health data and should support the Commission at EU level on the types of data, standards and specifications that are shared cross border and between healthcare providers at national level. Such standards and specifications should be detailed in EU legislation (delegated and implementing acts), moving beyond the voluntary guidelines currently in place. Additional work would be needed on tele-health and m-health, on quality, interoperability, security, access, portability and re-use of data, including by labelling, certification, authorisation, as per the first section of this report. This would also facilitate the provision of tele-health and m-health at national and EU level.
- Patients could be given access to the MyHealth@EU platform to increase their direct access to personal health data in a cross-border environment.
- Capacity building support provided by DG REFORM support should target Member States with lower level of readiness in adopting the different tools already developed (MyHealth@EU).
- Creating ad-hoc regulation to support the network initiatives (i.e. the MyHealth@EU platform) should be enhanced. The COVID-19 pandemic has emphasised the importance of public health and health data beyond the Member States borders. Setting compulsory standards and interoperability will not just benefit the patients but also the Digital Single Market, lowering the barriers to the free movement of digital healthcare products and services.

- Regulation should push for ensuring the use of the developed eID format on the MyHealth@EU platform as well as the adoption by Member States. Security should also be included among the tasks for national health authorities.
- Capacity building support provided by DG REFORM support should target Member States with lower level of readiness in adopting the different tools already developed (MyHealth@EU).
- To ensure better future evaluation of activities carried out in the area, eHealth Network members should be requested an accounting of their Man Days effort and other financial and non-financial inputs.
- To ensure the development of the European Health Data Space, the current structure of the eHealth Network should be revised as it is not able to address secondary use of data needs. A potential solution could be to have two different networks/groups/bodies, one focusing on primary use of data and involving the stakeholders currently addressed by the eHealth Network and the second one focusing on secondary use of data and involving data permit authorities as well as national data agencies. Such bodies would contribute to setting up at EU level the standards and specifications for quality, interoperability, security, access, portability and re-use of health data (for healthcare, research and policy making) and implement them at national level through labels, certifications etc. This would allow to fully coordinate the activities with all the stakeholders required. The activities of the two networks will need to be well coordinated to ensure lack of duplication and common use of certain tools and formats such as eID and interoperability standards. It will not make sense to disentangle the “production” of data from the “usage” of data. Together, the two networks will provide the two pillars on which to build European Health Data Space.
- eHealth Network activities should coordinate more with the different stakeholders with regards to:
 - DG RTD and DG CONNECT projects directly affecting the network objectives;
 - Data permit authorities, national health institutes (THEDAS JA);
 - Industry representatives.

7. References

- "21st Century Cures Act", PUBLIC LAW 114-255—DEC. 13, 2016
- Aceto, G. Persico, V. Pescape, A. (2018). The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges.
- Ahonen, O. Kouri, P. Kinnunen, UM. Junttila, K. Liljamo, P. Arifulla, D. Saranto, K. (2016). The Development Process of eHealth Strategy for Nurses in Finland.
- Ahuja A. S. (2019). The impact of artificial intelligence in medicine on the future role of the physician. *PeerJ*, 7, e7702.
- AI HLEG. (2019). Ethics Guidelines for trustworthy AI. AI High Level Expert Group, European Commission. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- Alami, H. Gagnon, M. P. Wootton, J.P. Zanaboni, P. (2017). Exploring factors associated with the uneven utilization of telemedicine in Norway: a mixed methods study.
- Alami, H., Lehoux, P., Auclair, Y., de Guise, M., Gagnon, M. P., Shaw, J., Roy, D., Fleet, R., Ahmed, M.A.A. & Fortin, J. P. (2020). Artificial Intelligence and Health Technology Assessment: Anticipating a New Level of Complexity. *Journal of medical Internet research*, 22(7), e17707.
- Albrecht, U.V. Kuhn, B. Land, J. Amelung, V.E. Von Jan, U. (2018). Assessing the benefits of digital health solutions in the societal reimbursement context.
- Alheit, K. (2001). The applicability of the EU product liability directive to software. *The comparative and international law journal of Southern Africa*, Vol. 34, No 2, pp. 188-209.
- Aluas, M., Maniac, V., Vaida, M. (2019). Using artificial intelligence in health: a call for legal regulation. *Applied Medical Informatics*, Vol. 41, Suppl. 1, 2019, p. 23.
- Alwon, BM. Solomon, G. Hussain, F. Wright, DJ. (2015). A detailed analysis of online pharmacy characteristics to inform safe usage by patients
- Angehrn, Z., Haldna, L., Zandvliet, A. S., Berglund, E. G., Zeeuw, J., Amzal, B., Cheung, S.A., Polasek, T.M., Pfister, M., Kerbusch, T. & Heckman, N. M. (2020). Artificial intelligence and machine learning applied at the point of care. *Frontiers in Pharmacology*, 11.
- Arak, P., Wójcik, A., & Polityka Insight. (2017). Transforming ehealth into a political and economic advantage (Rep.).
- Araújo, F.H.D., Santana, A.M., Santos Neto, P. de A. (2016). Using machine learning to support healthcare professionals in making preauthorisation decisions, *Int. J. Med. Inform.* 94, 1-7. doi: 10.1016/j.ijmedinf.2016.06.007.
- Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R. and Chatila, R. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, June 2020, Pages 82-115.
- Arrow, Kenneth J. (1963). Uncertainty and the Welfare Economics of Medical Care. *American Economic Review*. American Economic Association. 53 (5): 941–973.
- Arsene, O., Dumitache, I., Mihu, I. (2015). Expert system for medicine diagnosis using software agents. *Expert Systems with Applications*, 42(4): 1825-1834
- Asan, O., Bayrak, A. E., & Choudhury, A. (2020). Artificial intelligence and human trust in healthcare: Focus on clinicians. *Journal of medical Internet research*, 22(6), e15154.
- Auffray, C., Balling, R., Barroso, I. et al. (2016), Making sense of big data in health research: Towards an EU action plan. *Genome Med* 8, 71. <https://doi.org/10.1186/s13073-016-0323-y>

- Azzopardi-Muscat, N., Baeten, R., Clemens, T., Habicht, T., Keskimäki, I., Kowalska-Bobko, I., Sagan, A., & van Ginneken, E. (2018). The role of the 2011 patients' rights in cross-border health care directive in shaping seven national health systems: Looking beyond patient mobility. *Health policy* (Amsterdam, Netherlands), 122(3), 279–283. <https://doi.org/10.1016/j.healthpol.2017.12.010>
- Baig, M. A., Almuhaizea, M. A., Alshehri, J., Bazarbashi, M. S., & Al-Shagathrh, F. (2020). Urgent Need for Developing a Framework for the Governance of AI in Healthcare. *Studies in Health Technology and Informatics*, 272, 253-256.
- Barbour, A. B., Frush, J. M., Gatta, L. A., McManigle, W. C., Keah, N. M., Bejarano-Pineda, L., & Guerrero, E. M. (2019). Artificial Intelligence in Health Care: Insights From an Educational Forum. *Journal of Medical Education and Curricular Development*, 6, 2382120519889348.
- Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. *Health and Technology*, 7(4), 453–467. <https://doi.org/10.1007/s12553-017-0185-3>
- Benedict, M., Herrmann, H., Esswein, W. (2018). eHealth-Platforms - The Case of Europe. *Studies in health technology and informatics*. 247.
- Benjamins, S., Dhunnoo, P., & Meskó, B. (2020). The state of artificial intelligence-based FDA-approved medical devices and algorithms: an online database. *NPJ digital medicine*, 3(1), 1-8.
- Bensemmane, S. and Baeten, R. (2019), Cross-border telemedicine: practices and challenges. OSE Working Paper Series, Research Paper No.44 Brussels: European Social Observatory, October, 63p.
- Berger, M. L., Lipset, C., Gutteridge, A., Axelsen, K., Subedi, P., & Madigan, D. (2015). Optimizing the Leveraging of Real-World Data to Improve the Development and Use of Medicines. *Value in Health*, 18(1), 127–130. <https://doi.org/10.1016/j.jval.2014.10.009>
- Bernstein, J. A., Friedman, C., Jacobson, P., & Rubin, J. C. (2015). Ensuring public health's future in a national-scale learning health system. *American journal of preventive medicine*, 48(4), 480–487. <https://doi.org/10.1016/j.amepre.2014.11.013>
- Bhuyan, S. S., Bailey-DeLeeuw, S., Wyant, D. K., & Chang, C. F. (2016). Too Much or Too Little? How Much Control Should Patients Have Over EHR Data? *Journal of Medical Systems*, 40(7), 453–467. <https://doi.org/10.1007/s10916-016-0533-2>
- Bitterman, D. S., Aerts, H. J., & Mak, R. H. (2020). Approaching autonomy in medical artificial intelligence. *The Lancet Digital Health*, 2(9), e447-e449.
- Biundo, E., Pease, A., Segers, K., de Groote, M., d'Agent, T., & de Schaetzen, E. (2020). The socio-economic impact of ai in healthcare. Deloitte and MedTech Europe report. Retrieved from: <https://www.medtecheurope.org/resource-library/the-socio-economic-impact-of-ai-in-healthcare-addressing-barriers-to-adoption-for-new-healthcare-technologies-in-europe/>
- Blagec, K., Dorffner, G., Moradi, M., & Samwald, M. (2020). A critical analysis of metrics used for measuring progress in artificial intelligence. *arXiv preprint arXiv:2008.02577*.
- Blomberg SN, Folke F, Ersbøll AK, Christensen HC, Torp-Pedersen C, Sayre MR, Counts CR, Lippert FK. Machine learning as a supportive tool to recognize cardiac arrest in emergency calls, Resuscitation. 138 (2019) 322–329.
- Blumenthal S. The Use of Clinical Registries in the United States: A Landscape Survey. EGEMS (Wash DC). 2017;5(1):26. Published 2017 Dec 7. doi:10.5334/egems.248
- Bogaert, P., Van Oyen, H., & for BRIDGE Health (2017). An integrated and sustainable EU health information system: national public health institutes' needs and possible benefits. *Archives of public health = Archives belges de sante publique*, 75, 3. <https://doi.org/10.1186/s13690-016-0171-7>

- Bologna, G. & Hayashi, Y. (2017). Characterization of symbolic rules embedded in deep dimlp networks: A challenge to transparency of deep learning. *Journal of Artificial Intelligence and Soft Computing Research*, 7, 265–286.
- Bologna, S. Bellavista, A. Corso, PP. Zangara, G. (2016). Electronic Health Record in Italy and Personal Data Protection.
- Boogerd, E. Arts, T. Engelen, L. Van de Belt, T. (2015). "What Is eHealth": Time for An Update?
- Botrugno, C. (2019). Towards an ethics for telehealth.
- Bourassa Forcier, M., Gallois, H., Mullan, S., Joly, Y. (2019). Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policy makers? *Journal of Law and the Biosciences*, 317-335. DOI: 10.1093/jlb/lz013.
- Bouvet R., Desmarais, P. Minvielle, E. (2015). Legal and organizational barriers to the development of eHealth in France.
- Boyd, SE. Moore, LSP. Gilchrist, M. Costelloe, C. Castro-Sanchez, E. Franklin, BD. Holmes, AH. (2017). Obtaining antibiotics online from within the UK: a cross-sectional study.
- Bradford, L., Aboy, M., & Liddell, K. (2020). International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection. *Journal of Law and the Biosciences*, 7(1). <https://doi.org/10.1093/jlb/lzaa055>
- Brindusa M. (2018). Considerations regarding Directive 2011/24/EU on the application of patients' rights in cross-border healthcare in EU Member States. *Juridical Tribune (Tribuna Juridica)*, Bucharest Academy of Economic Studies, Law Department, vol. 8(3), pages 681-689, December.
- Buch, V. H., Ahmed, I., & Maruthappu, M. (2018). Artificial intelligence in medicine: current trends and future possibilities. *The British journal of general practice : the journal of the Royal College of General Practitioners*, 68(668), 143–144. <https://doi.org/10.3399/bjgp18X695213>
- Carter, S. M., Rogers, W., Win, K. T., Frazer, H., Richards, B., & Houssami, N. (2020). The ethical, legal and social implications of using artificial intelligence systems in breast cancer care. *The Breast*, 49, 25-32.
- Catan, G. Espanha, R. Mendes, RV. Toren, O. Chinitz, D. (2015). Health information technology implementation - impacts and policy considerations: a comparison between Israel and Portugal.
- Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': the US, EU, and UK approach. *Science and engineering ethics*, 24(2), 505-528.
- CB Insights Research Healthcare remains the hottest AI category for deals. 2017. <https://www.cbinsights.com/research/artificial-intelligence-healthcare-startups-investors/> (accessed 15 Jan 2018)
- Celegence (2020). Implications of MDR for Medical Devices Incorporating Artificial Intelligence and Machine Learning. Accessible via <https://www.celegence.com/implications-mdr-medical-devices-incorporating-artificial-intelligence-machine-learning/>
- Censi, F. Mattei, E. Triventi, M. Calcagnini, G (2015). Regulatory frameworks for mobile medical applications.
- Chagal-Feferkorn, K. (2019). AM I AN ALGORITHM OR A PRODUCT? When products liability should apply to algorithmic decision-makers. *Stanford Law and Policy Review*, 30 (61).
- Choy Flannigan, A. (2019). Legal and ethical issues with the use of AI in health & aged care. Retrieved from: <https://hallandwilcox.com.au/thinking/legal-and-ethical-issues-with-the-use-of-ai-in-health-aged-care/>

- Chronaki, C. Ploeg, F. (2016). Towards mHealth Assessment Guidelines for interoperability: HL7 FHIR.
- Cinasi, R.J., Zigrang, T.A., Bailey-Wheaton, J.L., Chen, D.J. (2017). Artificial Intelligence in Healthcare – Reimbursement. *Health Capital Topics*, 10(4).
- COCIR, the European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (2020). ARTIFICIAL INTELLIGENCE IN EU MEDICAL DEVICE LEGISLATION. September 2020.
- Codagnone, C., and F. Lupiáñez-Villanueva. (2013) "Benchmarking deployment of eHealth among general practitioners. Final report." European Union. Luxembourg. Publications Office of the European Union: European Commission. Directorate-General of Communications Networks. Content & Technology.
- Codagnone, C., and F. Lupiáñez-Villanueva. (2011) "A Composite Index for the Benchmarking of eHealth Deployment in European Acute Hospitals Distilling reality into a manageable form for evidence-based policy Strategic Intelligence Monitor on Personal Health Systems phase 2 (SIMPHS 2)." JRC-IPTS EUR 24825
- Cohen, I. G., Evgeniou, T., Gerke, S., & Minssen, T. (2020). The European artificial intelligence strategy: implications and challenges for digital health. *The Lancet Digital Health*, 2(7), e376-e379.
- Collins, G.S., Moons, K.G.M. (2019). Reporting of artificial intelligence prediction models. *The Lancet* Vol 393 April 20, 2019, 1577.
- Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic (2020) Official Journal of the European Union OJ L 227I , 16.7.2020, p. 1-9.
- Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (notified under document C(2019) 7460) (2020) Official Journal of the European Union OJ L 270, 24.10.2019, p. 83-93
- Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions eHealth action plan 2012-2020 - innovative healthcare for the 21st century (2012) Official Journal of the European Union
- Consiglio Superiore della Sanita in Italy (2017)
- Cortez, NG. Cohen, IG. Kesselheim, AS. (2014). FDA Regulation of Mobile Health Technologies
- Council conclusions on Health in the Digital Society — making progress in data-driven innovation in the field of health (2017) Official Journal of the European Union OJ JOC_2017_440_R_0005
- Crisan, O. (2017). Good pharmacy practice in the context of crossborder healthcare. *Farmacia*. 65. 310-316.
- Cuggia, M., & Combes, S. (2019). The French Health Data Hub and the German Medical Informatics Initiatives: Two National Projects to Promote Data Sharing in Healthcare. *Yearbook of medical informatics*, 28(1), 195–202. <https://doi.org/10.1055/s-0039-1677917>
- Cwiklicki, M. Schiavone, F. Klich, J. Pilch, K. (2020). Antecedents of use of eHealth services in Central Eastern Europe: a qualitative comparative analysis.
- Czeschik, Christina. (2018). Black Market Value of Patient Data. 10.1007/978-3-662-49275-8_78.
- Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. *Future healthcare journal*, 6(2), 94.

- De Backere, F., Bonte, P., Verstichel, S., Ongenae, F., & De Turck, F. (2018). Sharing health data in Belgium: A home care case study using the Vitalink platform. *Informatics for health & social care*, 43(1), 56–72. <https://doi.org/10.1080/17538157.2016.1269107>
- De Pietro, C., & Francetic, I. (2018). E-health in Switzerland: The laborious adoption of the federal law on electronic health records (EHR) and health information exchange (HIE) networks. *Health policy* (Amsterdam, Netherlands), 122(2), 69–74. <https://doi.org/10.1016/j.healthpol.2017.11.005>
- Delespaul, P. (2015). Routine outcome measurement in the Netherlands – A focus on benchmarking.
- Deloitte. (2021). *Digital transformation: Shaping the future of European healthcare*. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-shaping-the-future-of-european-healthcare.pdf>
- Den Exter, A. (2017). Chapter VII eHealth challenges under EU law.
- Den Exter, A., Santuari, A., Sokol, T. (2015). One Year after the EU Patient Mobility Directive: A Three-Country Analysis. *European law review*. 40. 279-293.
- Deo, R. C. (2015). Machine learning in medicine. *Circulation*, 132(20), 1920-1930. doi:10.1161/CIRCULATIONAHA.115.001593
- Diaz-Skeete, Y. Giggins, OM. McQuaid, D. Beaney, P. (2020). Enablers and obstacles to implementing remote monitoring technology in cardiac care: A report from an interactive workshop.
- Diebolt, V., Azancot, I., Boissel, F. H., Adenot, I., Balagué, C., Barthelemy, P., Boubenna, N., Coulonjou, H., Fernandez, X., Habran, E. & Lethiec, F. (2019). "Artificial intelligence": Which services, which applications, which results and which development today in clinical research? Which impact on the quality of care? Which recommendations?. *Therapies*, 74(1), 155-164.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016) Official Journal of the European Union OJ L 194, 19.7.2016, p. 1-30
- Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (2011) Official Journal of the European Union OJ L 88, 4.4.2011, p. 45–65.
- Dissent, D., "655,000 patient records for sale on the dark net after hacking victims refuse extortion demands," The Daily Dot, 27 01 2016. [Online]. Available: <http://www.dailydot.com/layer8/655000-patient-records-dark-net/>. [Accessed 06 05 2021].
- Dombai, P., Kis, M., Weber, I. (2014). Layman's version of the final report. Multiannual Work Plan 2015-2018 (JAseHn).
- Domergue, F., & Candore, G. (2020, September). The Data Analysis and Real-World Interrogation Network in the European Union (DARWIN EU) [ENCePP in the Time of Covid – Meeting]. <http://www.encepp.eu/publications/documents/14.FrancoisDomergueandGianmarioCandore-TheDataAnalysisandReal-WorldInterrogationNetworkinthe.pdf>
- Donahue, M. Bouhaddou, O. Hsing, N. Turner, T. Crandall, G. Nelson, J. Nebeker, J. (2018). Veterans Health Information Exchange: Successes and Challenges of Nationwide Interoperability.
- Drysdale, E., Dolatabadi, E., Corey Chivers, V. L., Such Saria, M. S. , Wiens, J., Brudno, M., Hoyt, A., Mazwi, M., Mamdani, M., Singh, D., Allen, V., McGregor, C., Ross, H., Szeto, A., Anand Verma, A., Wang, B., Paprica, P. A., & Goldenberg, A. (2020). Retrieved 6 April 2021, from <https://vectorinstitute.ai/wp-content/uploads/2020/03/implementing-ai-in-healthcare.pdf>

Ec.europa.eu, 27 November. As of 17 March 2017:

Edirippulige, S. Armfield, NR. (2017) Education and training to support the use of clinical telehealth: a review of the literature.

Eike-Henner Kluge¹, Paulette Lacroix², Pekka

EIT Health Consultative Group. (2020). Contribution to the discussion on the European Commission's Data Strategy and AI White Paper. Retrieved from: <https://eithealth.eu/wp-content/uploads/2020/06/EIT-Health-Consultative-Group-on-EC-Data-Strategy-and-AI-White-Paper-31-May-2020.pdf>

Enshaeifar, S., Zoha, A., Markides, A., Skillman, S., Acton, S.T., Elsaleh, T., Hassanpour, M., Ahrabian, A., Kenny, M., Klein, S., Rostill, H., Nilforooshan, R., Barnaghi, P. (2018). Health management and pattern analysis of daily living activities of people with dementia using in-home sensors and machine learning techniques, *PLoS One*, 13, 1–20. doi: 10.1371/journal.pone.0195605.

EPF's Response & Accompanying statement, 2020 - Public consultation on the White Paper on Artificial Intelligence.

EPF's Response Statement, 2021 - Public consultation on Data sharing in the EU – common European data spaces (new rules).

Esmaeilzadeh, P. (2020). Use of AI-based tools for healthcare purposes: a survey study from consumers' perspectives. *BMC medical informatics and decision making*, 20(1), 1-19.

Esteva, A., Robicquet, A., Ramsundar, B., Kuleshov, V., DePristo, M., Chou, K., Cui, C., Corrado, G., Thrun, S. & Dean, J. (2019). A guide to deep learning in healthcare. *Nature medicine*, 25(1), 24-29.

Ethayarajh, K., & Sadigh, D. (2020). BLEU Neighbors: A Reference-less Approach to Automatic Evaluation. *arXiv preprint arXiv:2004.12726*.

EU Commission. (2020). White Paper on Artificial Intelligence—A European Approach to Excellence and Trust, COM 65. Retrieved from: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

EU Parliament. (2020). Artificial Intelligence and Civil Liability: Legal Affairs. PE 621.926 - July 2020. Retrieved from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf).

European Commission (2018). COMMISSION STAFF WORKING DOCUMENT Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe. SWD 137 final.

European Commission 2014a. The Use of Big Data in Public Health Policy and Research. Ec.europa.eu,https://ec.europa.eu/health/ehealth/docs/ev_20141118_co07b_en.pdf

European Commission. (2012a). The Multiannual Work Plan 2012-2014 (eHGI JA). Brussels.

European Commission. (2012b). Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4188

European Commission. (2015). eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century.

European Commission. (2016a). eHealth Network GUIDELINE on Electronic exchange of health data under the Crossborder Directive 2011/24/EU. Retrieved from https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20160607_co05_03_en.pdf

- European Commission. (2016b). Study on Big Data in Public Health, Telemedicine and Healthcare. Retrieved from https://ec.europa.eu/health/sites/health/files/ehealth/docs/bigdata_report_en.pdf
- European Commission. (2017, October 6). EIF and ISA2 highlighted in new Ministerial Declaration on e-Government. ISA2 - European Commission. Retrieved from https://ec.europa.eu/isa2/news/european-interoperability-framework-and-isa%C2%B2-highlighted-new-ministerial-declaration-e_en
- European Commission. (2017). eHealth Network Multiannual Work Plan 2018-2021 (EHAction). Brussels.
- European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>
- European Commission. (2018a). Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services. Retrieved from https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co06_en.pdf
- European Commission. (2018b). Market study on telemedicine. Retrieved from https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf
- European Commission. (2019). EHealth adoption in primary healthcare in the EU is on the rise. Retrieved from <https://ec.europa.eu/digital-single-market/en/news/ehealth-adoption-primary-healthcare-eu-rise>
- European Commission. (2019). eHealth Network Guidelines to the EU Member States and the European Commission on an interoperable eco-system for digital health and investment programmes for a new/updated generation of digital infrastructure in Europe. [PDF]. Bucharest. Retrieved from https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co922_en.pdf
- European Commission. (2020). CEF Telecom - Innovation and Networks Executive Agency. Retrieved 30 October 2020, from <https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom>
- European Commission. (2020). eHealth DSI Operations. Retrieved from <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHealth+DSI+Operations+Home>
- European Commission. (2020). Electronic cross-border health services. Retrieved from https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en
- European Commission. (2021). *Assessment of the EU Member States' rules on health data in the light of GDPR.* https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf
- European Court of Auditors. (2019). Special Report: EU actions for cross-border healthcare: Significant ambitions but improved management required (Rep.).
- European Court of Auditors. (2020). EU actions for cross-border healthcare: significant ambitions but improved management required. Retrieved from: https://www.eca.europa.eu/Lists/ECADocuments/SR19_07/SR_HEALTH_CARE_EN.pdf
- European Investment Bank. (2019). Ireland: EIB confirms EUR 225 million backing for Irish eHealth programme. Retrieved from <https://www.eib.org/en/press/all/2018-249-eib-confirms-eur-225-million-backing-for-irish-ehealth-programme>
- European Medicines Agency. (2018). Data anonymisation - a key enabler for clinical data sharing (Vol. EMA/796532/2018, Rep.). arXiv:1712.05627 [cs.CY]
- European Medicines Agency. (2020). The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Purposes, A Discussion Paper for Medicines Developers,

- Data Providers, Research-Performing and Research-Supporting Infrastructures (Vol. EMA/194011/2020, Rep.).
- European Parliament (2020b). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. STOA. Panel for the Future of Science and Technology. Accessible via: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)
- European Parliament. (2020). Artificial Intelligence and Civil Liability. Retrieved from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf)
- European Regional and Local Health Authorities. (2020, March 24). Healthcare in Cross-Border regions. EUREGHA. <https://www.euregha.net/crossborderhealthcare/>
- European Society of Radiology (ESR). (2020). ESR Statement in response to European Commission White Paper on Artificial Intelligence – A European approach to excellence and trust. Retrieved from: https://www.myesr.org/sites/default/files/2020-06/esr_statement_for_public_consultation_artificial_intelligence_june2020.pdf
- European Union Agency for Cybersecurity. (2019, December 03). ENISA proposes Best Practices and Techniques for Pseudonymisation. Retrieved October, 2020, from <https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation>
- Expert Group on Liability and New Technologies. (2019) Liability for Artificial Intelligence and other emerging digital technologies. European Commission. Retrieved from: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>
- EY. (2019). Realising the value of health care data for a framework for the future. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/life-sciences/life-sciences-pdfs/ey-value-of-health-care-data-v20-final.pdf
- Eysenbach, G. (2001). What is eHealth?
- Fernández García, J., Spatharou, A., Hieronimus, S., Beck, J-P., & Jenkins, J. (2020). Transforming healthcare with AI. EIT Health and McKinsey & Company. Retrieved from: https://eithalth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf
- Flannigan, C. A. (2019). Legal and ethical issues with the use of AI in health & aged care. Health & Community Law Alert. Retrieved from: <https://hallandwilcox.com.au/thinking/legal-and-ethical-issues-with-the-use-of-ai-in-health-aged-care/>
- Fonseca, M. Karkaletsis, K. Cruz, I.A. Berler, A. Oliveira, I.C. (2015). OpenNCP: a novel framework to foster cross-border eHealth services.
- Food and Drug Administration. (2017). Digital Health Innovation Action Plan. <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf>
- Ford, E. W., Hesse, B. W., & Huerta, T. R. (2016). Personal Health Record Use in the United States: Forecasting Future Adoption Levels. Journal of Medical Internet Research, 18(3), e73. <https://doi.org/10.2196/jmir.4973>
- Frangez, D. Slak, B. (2016). Online counterfeit medicine trade in Slovenia.
- Gavrilov, G., Vlahu-Gjorgievska, E., & Trajkovik, V. (2020). Healthcare data warehouse system supporting cross-border interoperability. Health Informatics Journal, 26(2), 1321–1332. <https://doi.org/10.1177/1460458219876793>
- Gerke, S., Minssen, T., & Cohen, I. G. (2020). Ethical and Legal Challenges of Artificial Intelligence-Driven Health Care. Forthcoming in: Artificial Intelligence in Healthcare, 1st edition, Adam Bohr, Kaveh Memarzadeh (eds.).

- Gilbert, F. J., Smye, S. W., & Schönlieb, C. B. (2020). Artificial intelligence in clinical imaging: a health system approach. *Clinical Radiology*, 75(1), 3-6.
- Giuffrida, I. (2019). Liability for AI Decision-Making: Some Legal and Ethical Considerations. *Fordham L. Rev.*, 88, 439.
- Giunti, G. Guisado-Fernandez, E. Belani, H. Lacalle-Remigio, JR. (2019). Mapping the Access of Future Doctors to Health Information Technologies Training in the European Union: Cross-Sectional Descriptive Study.
- Glinkowski, WM. Karlinska, M. Karlinski, M. Krupinski, EA. (2018). Telemedicine and eHealth in Poland from 1995 to 2015.
- Gold, M. McLaughlin, C. (2016). Assessing HITECH Implementation and Lessons: 5 Years Later.
- Golding, L. P., & Nicola, G. N. (2019). A Business case for artificial intelligence tools: The currency of improved quality and reduced cost. *Journal of the American College of Radiology*, 16(9), 1357-1361.
- Gonçalves, M. A., Bayamlioglu, E., & Husovec, M. (2018). Liability arising from the use of Artificial Intelligence for the purposes of medical diagnosis and choice of treatment: who should be held liable in the event of damage to health?. Retrieved from: <http://arno.uvt.nl/show.cgi?fid=146408>
- Griebel, L. Enwald, H. Gilstad, H. Pohl, AL. Moreland, J. Sedlmayr, M. (2018). eHealth literacy research-Quo vadis?
- Gruson, D., Helleputte, T., Rousseau, P., & Gruson, D. (2019). Data science, artificial intelligence, and machine learning: opportunities for laboratory medicine and the value of positive regulation. *Clinical biochemistry*, 69, 1-7.
- Haas-Wilson, D. (2001). Arrow and the Information Market Failure in Health Care: The Changing Content and Sources of Health Care Information. *Journal of Health Politics, Policy and Law*, 26(5), 1031-1044. <https://doi.org/10.1215/03616878-26-5-1031>
- Habli, I., Lawton, T., & Porter, Z. (2020). Artificial intelligence in health care: accountability and safety. *Bulletin of the World Health Organization*, 98(4), 251.
- Hacker, P. (2018). Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, 55(4), 1143-1185.
- Hackett, C., Brennan, K., Smith Fowler, H., & Leaver, C. (2019). Valuing Citizen Access to Digital Health Services: Applied Value-Based Outcomes in the Canadian Context and Tools for Modernizing Health Systems. *Journal of Medical Internet Research*, 21(6), e12277. <https://doi.org/10.2196/12277>
- Handelman, G. S., Kok, H. K., Chandra, R. V., Razavi, A. H., Huang, S., Brooks, M., ... & Asadi, H. (2019). Peering into the black box of artificial intelligence: evaluation metrics of machine learning methods. *American Journal of Roentgenology*, 212(1), 38-43.
- Harbers M., Peeters M.M.M., Neerincx M.A. "Perceived Autonomy of Robots: Effects of Appearance and Context" in ALDINHAS FERREIRA, MI, SILVA SEQUEIRA, J., TOKHI, MO, KADAR, E., Y VIRK, GS (EDS.), *A World with Robots*, Springer, Cham, 2017, pp. 19-33.
- Haux, R. Ammenwerth, E. Koch, S. Lehmann, CU. Park, HA. Saranto, K. Wong, CP. (2018). A Brief Survey on Six Basic and Reduced eHealth Indicators in Seven Countries in 2017.
- Heads of Medicines Agency & European Medicines Agency. (2020). HMA-EMA Joint Big Data Taskforce Phase II report: 'Evolving Data-Driven Regulation.' https://www.ema.europa.eu/en/documents/other/hma-ema-joint-big-data-taskforce-phase-ii-report-evolving-data-driven-regulation_en.pdf
- Heinze, O., Birkle, M., Köster, L., & Bergh, B. (2011). Architecture of a consent management suite and integration into IHE-based regional health information networks. *BMC Medical Informatics and Decision Making*, 11(1). <https://doi.org/10.1186/1472-6947-11-58>

- Hern, A. (2019, July 23). 'Anonymised' data can never be totally anonymous, says study. Retrieved October, 2020, from <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds>
- Herzog, J. Sauermann, S. Mense, A. Forjan, M. Urbauer, P. (2015). Development of Knowledge Profiles for International eHealth eLearning Courses.
- High-Level Expert Group on Artificial Intelligence (HLEG). (2019). Ethics guidelines for trustworthy AI. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- Ho, C. W. L., Soon, D., Caals, K., & Kapur, J. (2019). Governance of automated image analysis and artificial intelligence analytics in healthcare. *Clinical radiology*, 74(5), 329-337.
- Hollmark, M. Lefevre Skjoldebrand, A. Andersson, C. Lindblad, R. (2015). Technology Ready to be Launched, but is there a Payer? Challenges for Implementing eHealth in Sweden.
- Holzinger, A., Dehmer, M., & Jurisica, I. (2014). Knowledge discovery and interactive data mining in bioinformatics—State-of-the-art, future challenges and research directions. *BMC Bioinformatics*, 15, I1.
- Horgan, D., Romao, M., Morré, S. A., & Kalra, D. (2019). Artificial Intelligence: Power for Civilisation—and for Better Healthcare. *Public Health Genomics*, 22(5-6), 145-161.
- <https://ec.europa.eu/digital-single-market/en/news/discussion-big-data-and-healthcare-new-knowledge-era-world-healthcare>
- Hueso, L. (2019). Ethics in Design for the Development of an Artificial Intelligence, Trustworthy Robotics and Big Data and their Utility for the Law. *Revista catalana de dret public*, 58.
- iHD & Digital Health Society. (2021). Calls to Action on Health Data Ecosystems. <https://www.i-hd.eu/wp-content/uploads/2021/03/Calls-to-Action-on-Health-Data-Ecosystems-2021-DHE-IHD-.pdf>
- J Borej, M Cabrnnoch, J Geier, T Bezouska. (2019, September). Report on best practices and approaches on data protection at national level (Version 0.7a, 26/09/2019). coFunded by the European Union's Health Programme Grant Agreement no 801558. http://ehaction.eu//wp-content/uploads/2020/05/3.1_D7.2-Best-practices-report-on-data-protection-at-national-level-eHAction_16th-eHN_ANEX.pdf
- Jack, A. (2016). Can anyone stop the illegal sale of medicines online?
- Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H. & Wang, Y. (2017). Artificial intelligence in healthcare: past, present and future. *Stroke and vascular neurology*, 2(4), 230-243.
- Jogova, M. Shaw, J. Jamieson, T. (2019). The Regulatory Challenge of Mobile Health: Lessons for Canada.
- Katehakis, DG. Masi, M. Wisniewski, F. Bittins, S. (2016). Towards a Cross-domain Infrastructure to Support Electronic Identification and Capability Lookup for Cross-border ePrescription/Patient Summary Services.
- Kautsch, M. Lichon, M. Matuszak, N. (2017). Setting the scene for the future: implications of key legal regulations for the development of eHealth interoperability in the EU.
- Kelly, C. J., Karthikesalingam, A., Suleyman, M., Corrado, G., & King, D. (2019). Key challenges for delivering clinical impact with artificial intelligence. *BMC medicine*, 17(1), 195.
- Kierkegaard, P. (2015). Governance structures impact on eHealth.

- Kluge, EH. Lacroix, P. Ruotsalainen, P. (2018). Ethics Certification of Health Information Professionals
- Kluge, EW. (2017). Health Information Professionals in a Global eHealth World: Ethical and legal arguments for the international certification and accreditation of health information professionals.
- Kolasa, K. Kozinski, G. (2020). How to Value Digital Health Interventions? A Systematic Literature Review
- Kouroubali, A., & Katehakis, D. G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of biomedical informatics*, 94, 103166. <https://doi.org/10.1016/j.jbi.2019.103166>
- Laï, M. C., Brian, M., & Mamzer, M. F. (2020). Perceptions of artificial intelligence in healthcare: findings from a qualitative survey study among actors in France. *Journal of Translational Medicine*, 18(1), 1-13.
- LaRosa, E., & Danks, D. (2018, December). Impacts on trust of healthcare AI. In Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society (pp. 210-215).
- Larrucea, X., Moffie, M., Asaf, S., & Santamaria, I. (2020). Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Computer Standards & Interfaces*, 69, 103408. <https://doi.org/10.1016/j.csi.2019.103408>
- Larsen, SB. Sorensen, NS. Petersen, MG. Kjeldsen, GF. (2016). Towards a shared service centre for telemedicine: Telemedicine in Denmark, and a possible way forward
- Lin, CC. Dievler, A. Robbins, C. Sripiatana, A. Quinn, M. Nair, S. (2018). Telehealth In Health Centers: Key Adoption Factors, Barriers, And Opportunities.
- Liyanage, H., Liaw, S. T., Jonnagaddala, J., Schreiber, R., Kuziemsky, C., Terry, A. L., & de Lusignan, S. (2019). Artificial Intelligence in Primary Health Care: Perceptions, Issues, and Challenges: Primary Health Care Informatics Working Group Contribution to the Yearbook of Medical Informatics 2019. *Yearbook of medical informatics*, 28(1), 41.
- Luo, L., Liao, C., Zhang, F., Zhang, W., Li, C., Qiu, Z., Huang, D. (2018). Applicability of internet search index for asthma admission forecast using machine learning, *Int. J. Health Plann. Manage*, 33, 723–732. doi:10.1002/hpm.2525.
- Macrae, C. (2019). Governing the safety of artificial intelligence in healthcare. *BMJ quality & safety*, 28(6), 495-498.
- Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R., Thota, C. (2018). A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system, *Futur. Gener. Comput. Syst.*, 82, 375–387. doi: 10.1016/j.future.2017.10.045.
- Mantovani, E. Bocos, PC. (2017). Are mHealth Apps Safe? The Intended Purpose Rule, Its Shortcomings and the Regulatory Options Under the EU Medical Device Framework.
- March 2018 Independent Performance Evaluation, Canada Health Infoway
- Marian, B. (2018). Considerations regarding Directive 2011/24/EU on the application of patients' rights in cross-border healthcare in EU Member States (3rd ed., Vol. 8, pp. 681-689, Publication). *Juridical Tribune*.
- Marjanovic, S., Ghiga, I., Yang, M., & Knack, A. (2017). Understanding value in health data ecosystems: A review of current evidence and ways forward. https://www.rand.org/pubs/research_reports/RR1972.html.
- Martínez, R. (2019). Designing Artificial Intelligence. Challenges and Strategies for Achieving Regulatory Compliance (Es-En). *Revista catalana de dret públic*, 64-81.
- Martins, H. (2014). Temporary legal agreement (TLA) to upkeep epSOS developed cross border eHealth services.

- Martins, H. (2021). Digital Healthcare Focus: liability issues of AI use in Healthcare. Accessible via <https://healthmanagement.org/c/it/post/digital-healthcare-focus-liability-issues-of-ai-use-in-healthcare>
- Mazor, K. M., Richards, A., Gallagher, M., Arterburn, D. E., Raebel, M. A., Nowell, W. B., Curtis, J. R., Paolino, A. R., & Toh, S. (2017). Stakeholders' views on data sharing in multicenter studies. *Journal of Comparative Effectiveness Research*, 6(6), 537–547. <https://doi.org/10.2217/cer-2017-0009>
- McCarthy, J. (2007). From here to human-level AI. *Artificial Intelligence*, 171(18), 1174-1182.
- Medical Informatics Initiative Germany. (2018, July 5). BMBF provides funding for the Medical Informatics Initiative. Retrieved October, 2020, from <https://www.medizininformatik-initiative.de/en/bmbf-provides-funding-medical-informatics-initiativ>
- Mehta, N., Pandit, A., & Shukla, S. (2019). Transforming healthcare with big data analytics and artificial intelligence: A systematic mapping study. *Journal of Biomedical Informatics*, 100, 103311.
- Merkel, S., & Hess, M. (2020). The Use of Internet-Based Health and Care Services by Elderly People in Europe and the Importance of the Country Context: Multilevel Study. *JMIR Aging*, 3(1), e15491. <https://doi.org/10.2196/15491>
- Meyer, Z. D., Pfahringer, B., Kempfert, J., Kuehne, T., Sündermann, S.H., Stamm, C., Hofmann, T., Falk, V., Eickhoff, C. (2018). Machine learning for real-time prediction of complications in critical care: a retrospective study, *Lancet Respir. Med.*, 6, 905–914. doi: 10.1016/S2213-2600(18)30300-X.
- Miro Llinares, F. (2018). Artificial intelligence and criminal justice: beyond the harmful results caused by Robots. *Journal of Criminal Law and Criminology*, 3rd Epoch, No. 20, pp. 87-130.
- Morris, C. Scott, R. Mars, M. (2019). Security and Other Ethical Concerns of Instant Messaging in Healthcare.
- Mouton Dorey, C., Baumann, H., & Biller-Andorno, N. (2018). Patient data and patient rights: Swiss healthcare stakeholders' ethical awareness regarding large patient data sets - a qualitative study. *BMC medical ethics*, 19(1), 20. <https://doi.org/10.1186/s12910-018-0261-x>
- Mucic, D. (2008). International telepsychiatry: a study of patient acceptability.
- Muehlematter, U. J., Daniore, P., & Vokinger, K. N. (2021). Approval of artificial intelligence and machine learning-based medical devices in the USA and Europe (2015–20): a comparative analysis. *The Lancet Digital Health*, 3(3), e195–e203. DOI: [https://doi.org/10.1016/S2589-7500\(20\)30292-2](https://doi.org/10.1016/S2589-7500(20)30292-2)
- Nacinovich, M. 2011. "Defining mHealth," *Journal of Communication in Healthcare* (4:1), pp. 1-3. OWL 2 Web Ontology
- Nalin, M. Baroni, I. Faiella, G. Romano, M. Matrisciano, F. Gelenbe, E. Martinez, DM. Dumortier, J. Natsiavas, P. Votis, K. Koutkias, V. Tzovaras, D. Clemente, F. (2019). The European cross-border health data exchange roadmap: Case study in the Italian setting. *Journal of Biomedical Informatics*.
- Natsiavas, P. Rasmussen, J. Voss-Knude, M. Votis, K. Coppolino, L. Campegiani, P. Cano, I. Mari, D. Faiella, G. Clemente, F. Nalin, M. Grivas, E. Stan, O. Gelenbe, E. Dumortier, J. Petersen, J. Tzovaras, D. Romano, L. Komnios, I. Koutkias, V (2018). Comprehensive user requirements engineering methodology for secure and interoperable health data exchange.
- Natsiavas, P., Kakalou, C., Votis, K., Tzovaras, D., Koutkias, V. (2019). Citizen Perspectives on Cross-Border eHealth Data Exchange: A European Survey. *Studies in health technology and informatics*. 264. 719-723. 10.3233/SHTI190317.
- NG, A. (2021) Deep Learning AI. <https://www.deeplearning.ai/the-batch/issue-80/>

- Nieszporska, S. (2016). Priorities in the Polish health care system. *The European Journal of Health Economics*. 18. 10.1007/s10198-016-0831-0.
- Odone, A., Buttigieg, S., Ricciardi, W., Azzopardi-Muscat, N., & Staines, A. (2019). Public health digitalization in Europe: EUPHA vision, action and role in digital public health. *European journal of public health*, 29 (Supplement_3), 28-35.
- OECD (2019), Recommendation of the Council on Health Data Governance, OECD/LEGAL/0433
- OECD (2019). Using routinely collected data to inform pharmaceutical policies. Analytical Report for OECD and EU countries.
- OECD (2020). Trustworthy AI in Health: Background paper for the G20 AI Dialogue, Digital Economy Task Force. Retrieved from: <https://www.oecd.org/health/trustworthy-artificial-intelligence-in-health.pdf>
- OECD, Slawomirski, L., A. Auroraen and N. Klazinga (2017), "The economics of patient safety: Strengthening a value-based approach to reducing patient harm at national level", OECD Health Working Papers, No. 96, OECD Publishing, Paris, <https://doi.org/10.1787/5a9858cd-en>.
- Oh, H. Rizo, C. Enkin, M. Jadad, A. (2005). What Is eHealth (3): A Systematic Review of Published Definitions
- Olimid, AP. Olimid, DA. (2019). Ethical assessment of the EU health policy under the Directive 2011/24/EU: approaching patients' rights and cross-border healthcare.
- Oliver, A. J. (2000). Internet pharmacies: Regulation of a growing industry.
- Ordish, J. (2018). Legal liability for machine learning in healthcare. PHG Foundation. Accessible via: <https://www.phgfoundation.org/briefing/legal-liability-machine-learning-in-healthcare>
- Otto, L. Harst, L. Schlieter, H. Wollschlaeger, B. Richter, P. Timpel, P. (2018). Towards a Unified Understanding of eHealth and Related Terms – Proposal of a Consolidated Terminological Basis.
- Panteli, D., Wagner, C., Verheyen, F., Busse, R. (2015). Continuity of care in the cross-border context: insights from a survey of German patients treated abroad. *European journal of public health*, 25(4), 557–563. <https://doi.org/10.1093/eurpub/cku251>
- Paranjape, K., Schinkel, M., & Nanayakkara, P. (2020). Short Keynote Paper: Mainstreaming Personalized Healthcare—Transforming Healthcare Through New Era of Artificial Intelligence. *IEEE journal of biomedical and health informatics*, 24(7), 1860-1863.
- Parker, L. Halterb, V. Karliychukc, T. Grundy, Q. (2019). How private is your mental health app data? An empirical study of mental health app privacy policies and practices.
- Parkes, D. C., & Wellman, M. P. (2015). Economic reasoning and artificial intelligence. *Science*, 349(6245), 267-272.
- Parv, L. Kruus, P., Motte, K. Roos, P. (2014). An evaluation of e-prescribing at a national level.
- Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. *Insights into imaging*, 9(5), 745-753.
- Pham, T., Tran, T., Phung, D., Venkatesh, S. (2017). Predicting healthcare trajectories from medical records: A deep learning approach, *J. Biomed. Inform.* 69, 218–229. doi: 10.1016/j.jbi.2017.04.001.
- Pohlmann, S. Kunz, A. Ose, D. Winkler, EC. Brandner, A. Poss-Doering, R. Szecsenyi, J. Wensing, M. (2020). Digitalizing Health Services by Implementing a Personal Electronic Health Record in Germany: Qualitative Analysis of Fundamental Prerequisites From the Perspective of Selected Experts.
- Price, W. N., Gerke, S., & Cohen, I. G. (2019). Potential liability for physicians using artificial intelligence. *Jama*, 322(18), 1765-1766.

- Prior, L. (2003). Belief, knowledge and expertise: the emergence of the lay expert in medical sociology. *Sociology of Health & Illness*, 25(3), 41–57. <https://doi.org/10.1111/1467-9566.00339>
- Quinn, P. (2017). The EU commission's risky choice for a non-risk based strategy on assessment of medical devices.
- Rai, A. (2020). Explainable AI: From black box to glass box. *Journal of the Academy of Marketing Science*, 48(1), 137–141.
- Recht, M. P., Dewey, M., Dreyer, K., Langlotz, C., Niessen, W., Prainsack, B., & Smith, J. J. (2020). Integrating artificial intelligence into the clinical practice of radiology: challenges and recommendations. *European Radiology*, 1–9.
- Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. *Journal of the American Medical Informatics Association*, 27(3), 491–497.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU (2016) Official Journal of the European Union OJ L 119, 4.5.2016, p. 1–88
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (2017) Official Journal of the European Union OJ L 117, 5.5.2017
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014) Official Journal of the European Union OJ L 257, 28.8.2014, p. 73–114
- Reutiman, J.L. (2012). Defective information: Should Information be a product subject to product liability claims? *Cornell Journal of Law and Public Policy*. Volume 22, Issue 1, Fall 2012.
- Riedel, R. (2016). Patient's Cross-border Mobility Directive: Application, Performance and Perceptions Two Years after Transposition. *Baltic Journal of European Studies*. 6. 10.1515/bjes-2016-0012.
- Rohatgi, J. (2018, December 17). GDPR and healthcare: Understanding health data and consent. Retrieved September, 2020, from <https://www.pega.com/insights/articles/gdpr-and-healthcare-understanding-health-data-and-consent>
- Ross, J., Stevenson, F., Lau, R., & Murray, E. (2016). Factors that influence the implementation of e-health: a systematic review of systematic reviews (an update). *Implementation science : IS*, 11(1), 146. <https://doi.org/10.1186/s13012-016-0510-7>
- Rossi, F. (2016). Artificial intelligence: Potential benefits and ethical considerations. European parliament briefing PE, 571.380. Retrieved from: [http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI\(2016\)571380_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/571380/IPOL_BRI(2016)571380_EN.pdf).
- Rowley, A., Turpin, R. & Walton, S. (2019). The emergence of artificial intelligence and machine learning algorithms in healthcare: Recommendations to support governance and regulation. Retrieved from: <https://www.bsigroup.com/globalassets/localfiles/en-gb/about-bsi/nsb/innovation/mhra-ai-paper-2019.pdf>

- Rutledge, C. Kott, K. Schweickert, P. Poston, R. Fowler, C. Haney, T. (2017). Telehealth and eHealth in nurse practitioner training: current perspectives.
- Sabes-Figuera, Ramon, and I. Maghiros. (2013) "European hospital survey: benchmarking deployment of e-Health services (2012–2013)." European Comission
- Schaefer, E. Schnell, G. Sonsalla, J. (2015). Obtaining reimbursement in France and Italy for new diabetes products.
- Schiza, E. C., Kyprianou, T. C., Petkov, N., Schizas, C. N. (2019). Proposal for an eHealth Based Ecosystem Serving National Healthcare. IEEE journal of biomedical and health informatics, 23(3), 1346–1357. <https://doi.org/10.1109/JBHI.2018.2834230> Better Regulation Toolbox, tool 46
- Schnell-Inderst, P. Mayer, J. Lauterberg, J. Hunger, T. Arvandi, M. Conrads-Frank, A. Nachtnebel, A. Wild, C. Siebert, U. (2015). Health technology assessment of medical devices: What is different? An overview of three European projects.
- Schönberger, D. (2019). Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications. International Journal of Law and Information Technology, 27(2), 171–203.
- Schoppe, K. (2018). Artificial intelligence: who pays and how?. Journal of the American College of Radiology, 15(9), 1240-1242.
- Schulz S., Stegwee R., Chronaki C. (2019). Standards in Healthcare Data.
- Shaw, J., Rudzicz, F., Jamieson, T., & Goldfarb, A. (2019). Artificial intelligence and the implementation challenge. Journal of Medical Internet Research, 21(7), e13659.
- Shinners, L., Aggar, C., Grace, S., & Smith, S. (2020). Exploring healthcare professionals' understanding and experiences of artificial intelligence technology use in the delivery of healthcare: An integrative review. Health informatics journal, 26(2), 1225-1236.
- Sloan, F. A. (2001). Arrow's Concept of the Health Care Consumer: A Forty-Year Retrospective. Journal of Health Politics, Policy and Law, 26(5), 899–912. <https://doi.org/10.1215/03616878-26-5-899>
- Soni, N., Sharma, E. K., Singh, N., & Kapoor, A. (2020). Artificial intelligence in business: from research and innovation to market deployment. Procedia Computer Science, 167, 2200–2210.
- Sood, S. Mbarika, V. Jugoo, S. Dookhy, R. Doarn, C.R. Prakash, N. Merrell, R.C. (2007). What Is Telemedicine? A Collection of 104 Peer-Reviewed Perspectives and Theoretical Underpinnings.
- Spagnuelo, D. Lenzini, G. (2017). Transparent Medical Data Systems.
- Spencer, K., Sanders, C., Whitley, E. A., Lund, D., Kaye, J., & Dixon, W. G. (2016). Patient Perspectives on Sharing Anonymized Personal Health Data Using a Digital System for Dynamic Consent and Research Feedback: A Qualitative Study. Journal of medical Internet research, 18(4), e66. <https://doi.org/10.2196/jmir.5011>
- Srinivasan, U. (2017, July 05). Primary and Secondary Uses of Health Data. Retrieved October, 2020, from <https://flyingblind.cmcrc.com/researchers/primary-and-secondary-uses-health-data>
- Stanfill, M. H., & Marc, D. T. (2019). Health information management: implications of artificial intelligence on healthcare data and information management. Yearbook of medical informatics, 28(1), 56.
- Strohm, L., Hehakaya, C., Ranschaert, E. R., Boon, W. P., & Moors, E. H. (2020). Implementation of artificial intelligence (AI) applications in radiology: hindering and facilitating factors. European Radiology.

- Sullivan, H. R., & Schweikart, S. J. (2019). Are current tort liability doctrines adequate for addressing injury caused by AI?. *AMA journal of ethics*, 21(2), 160-166.
- Sun, T. Q., & Medaglia, R. (2019). Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare. *Government Information Quarterly*, 36(2), 368-383.
- Tang, A., Tam, R., Cadrin-Chênevert, A., Guest, W., Chong, J., Barfett, J., Chepelev, L., Cairns, R., Mitchell, J.R., Cicero, M.D. & Poudrette, M. G. (2018). Canadian Association of Radiologists white paper on artificial intelligence in radiology. *Canadian Association of Radiologists Journal*, 69(2), 120-135.
- Tinholz, D., van Niel, E., van Kraaij, C., & Knödler, M. (2017). Artificial intelligence benchmark. Capgemini Consulting. Retrieved from: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Artificial+Intelligence+Benchmark+capgemini&btnG=
- Tsioumanis, V. Mangita, A. Diomidous, M. (2016). Applications and Developments of Telemedicine in Greece.
- Tzanetakos, G. Ullrich, F. Meuller, K. (2017). Telepharmacy Rules and Statutes: A 50-State Survey.
- Van Hartskamp, M., Consoli, S., Verhaegh, W., Petkovic, M., & Van de Stolpe, A. (2019). Artificial intelligence in clinical health care applications. *Interactive Journal of Medical Research*, 8(2), e12100.
- Van Houwelingen, CTM. Moerman, AH. Ettema, RGA. Kort, HSM. ten Cate, O. (2016). Competencies required for nursing telehealth activities: A Delphi-study.
- Van Leeuwen, K.G., Schalekamp, S., Rutten, M.J., van Ginneken, B. and de Rooij, M. (2021). Artificial intelligence in radiology: 100 commercially available products and their scientific evidence. *European radiology*, 31(6), pp.3797-3804.
- Vellido, A. (2019). Societal issues concerning the application of Kidney Diseases, 5(1), 11-17.
- Verheij, R.A., Curcin, V., Delaney, B.C., & McGilchrist, M.M. (2018). Possible sources of bias in primary care electronic health record data use and reuse. *Journal of medical Internet research*, 20(5), e185.
- Verra, S., Kroese, R., Ruggeri, K. (2016). Facilitating safe and successful cross-border healthcare in the European Union. *Health Policy*. 120. 10.1016/j.healthpol.2016.04.014.
- Von Wedel, P., & Hagist, C. (2020). Economic Value of Data and Analytics for Health Care Providers: Hermeneutic Systematic Literature Review. *Journal of medical Internet research*, 22(11), e23315.
- Walker,D, (2014). "Research examines cost of stolen data, underground services'," SC Magazine.
- Wang, S. Y., Pershing, S., & Lee, A. Y. (2020). Big data requirements for artificial intelligence. *Current Opinion in Ophthalmology*, 31(5), 318-323.
- WHO Global Observatory for eHealth, mHealth. (2011). New horizons for health through mobile technologies. www.who.int/goe/publications/goe_mHealth_web.pdf
- Wilson, K., & Khansa, L. (2018). Migrating to electronic health record systems: A comparative study between the United States and the United Kingdom. *Health policy* (Amsterdam, Netherlands), 122(11), 1232-1239. <https://doi.org/10.1016/j.healthpol.2018.08.013>
- Wiring, R. (2018). Digitisation in Healthcare: from Utopia to Reality – Artificial Intelligence, its Legal Risks and Side Effects. CMS lawyers. Retrieved from: Digitisation of healthcare: key legal issues around AI | International law firm CMS

Wolff, J., Pauling, J., Keck, A., & Baumbach, J. (2020). The Economic Impact of Artificial Intelligence in Health Care: Systematic Review. *Journal of Medical Internet Research*, 22(2), e16866.

Yu, K. H., Beam, A. L., & Kohane, I. S. (2018). Artificial intelligence in healthcare. *Nature biomedical engineering*, 2(10), 719-731.

Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, 1-22.

8. Annex

8.1 Research questions

8.1.1 Digital health products and services

Table 56. Digital health products and services initial research questions

Area	Research questions (RQ)
Definitions (A1)	<p>What are the existing or future (planned) national rules on the definition of telehealth (or similar concepts) and its scope, namely on what is telehealth and which services are deemed to fall within its scope?</p> <p>What are the existing or future (planned) national rules on the definition of telemedicine (or similar concepts) and its scope, namely national rules defining what is telemedicine and which services are deemed to fall within its scope?</p> <p>What are the existing or future (planned) national rules on the definition of mHealth (or similar concepts) and its scope, namely on what is mHealth and which services are deemed to fall within its scope?</p>
Approval, certification, authorisation and reimbursement rules that can impact on free movement of digital health services and products (A2)	<p>What are the existing or future (planned) national rules (including non-legislative measures) for the approval, certification or authorisation of eHealth services and products (including mHealth, AI, telehealth and telemedicine) and their potential impact on the cross-border provision and free movement of these services and products?</p> <p>What are the existing or future (planned) national rules (including non-legislative measures) for the approval, certification or authorisation of eHealth services and products (including mHealth, AI, telehealth and telemedicine) and their potential impact on the functioning of the internal market?</p> <p>What are the existing or future (planned) national rules regulating eHealth services and products (including mHealth, AI, telehealth and telemedicine) practices, reimbursement, pricing and HTA and their potential impact on the cross-border provision and free movement of these services and products?</p> <p>What are the existing or future (planned) national rules regulating eHealth services and products (including mHealth, AI, telehealth and telemedicine) practices, reimbursement, pricing and HTA and their potential impact on the functioning of the internal market?</p> <p>What are the cost and benefits of harmonising or not the rules concerning the approval, certification, authorisation and reimbursement of telehealth and mHealth systems at EU level?</p> <p>What measures, from the perspective of existing rules (article 7 of the Directive 2011/24/EU, regulated professions directive, etc.), should be taken at EU level concerning the approval, certification, authorisation and reimbursement of telehealth and mHealth systems at EU level?</p>
Interoperability between mHealth, telehealth and electronic health records/registries, and interoperability with other IoT (A3)	<p>What are the existing or future (planned) national rules or guidance on the interoperability of patients' data generated by mHealth tools and medical devices with electronic health records/registries and other databases and their potential impact on the cross-border provision and free movement of these services and products in the internal market?</p> <p>What are the standards used for the interoperability of telehealth/mHealth applications (including those that are medical devices) and electronic health records/registries, as well as with other systems in health area in Member States and are the impact of divergent standards on the free movement of digital health services between Member States?</p> <p>What are the existing or future (planned) national rules concerning the possibility for patients to request the transfer of data from mobile applications (wellbeing applications, apps prescribed or non-prescribed by healthcare professional, and including medical devices) into electronic health records and the extent of their implementation and their technical implications?</p> <p>What are the advantages deriving from the implementation of interoperability between telehealth/mHealth (including medical devices) and electronic health records/registries and of any costs entailed by the lack of interoperability?</p> <p>What are the existing or future (planned) national rules concerning the interoperability and transfer of data between Internet of Things (IoT) applications, medical devices, mHealth and telehealth tools; the type of data transferred with IoT (personal, non-personal, etc.) and the rules in this respect?</p> <p>What are the cost and benefits of harmonising or not the rules concerning interoperability of telehealth and mHealth systems at EU level?</p>

Area	Research questions (RQ)
	<p>What measures should be taken at EU level concerning interoperability of telehealth and mHealth systems at EU level?</p> <p>What are the existing or future (planned) national rules on safety and liability for eHealth (with a special focus on mHealth and telehealth) services and products and their potential impact on the functioning of the internal market?</p> <p>What measures that should be taken at EU level in order to counteract the impact on the cross-border provision and circulation of these services and products?</p> <p>What measures that should be taken at EU level in order to counteract the impact on the functioning of the internal market?</p> <p>Are there transparency issues regarding the applicable liability rules and consequent confidence/uncertainty of the providers, healthcare professionals and patients?</p> <p>What are the existing or future (planned) national rules or guidance concerning the digital authentication and authorisation of patients and healthcare providers in the context of mHealth?</p> <p>What are the existing or future (planned) national rules or guidance (e.g. codes of conduct) on privacy and data protection aspects of mHealth products/apps?</p> <p>What are the costs and benefits of harmonising (or not) the rules concerning the privacy and liability rules of telehealth and mHealth systems at EU level? (in terms of efficiency, societal costs, etc.)</p>
Professional qualifications for providing telehealth services (A5)	<p>What are the existing or future (planned) national rules establishing the necessary requirements for professional qualifications or quality standards for the provision of telehealth services and their potential impact on the cross-border provision of telehealth services?</p> <p>What is the level of cross-border recognition of professional qualifications for healthcare professionals in the context of telehealth/mHealth? (with particular focus on the specific national requirements for healthcare professionals providing telehealth services to patients who are established in another Member States)</p> <p>What is the level of recognition of telehealth in guidance documents for healthcare professionals including clinical guidelines and other Member States' recommendations on telehealth?</p> <p>Are there different rules between Member States in terms of professional qualifications for telehealth/mHealth professionals?</p> <p>How the different rules between Member States in terms of professional qualifications for telehealth/mHealth professionals impact the functioning of the internal market?</p> <p>What measures should be taken at EU level in order to counteract this impact concerning the different rules between Member States in terms of professional qualifications for telehealth/mHealth professionals?</p> <p>What are the costs and benefits of harmonising (or not) the rules concerning the professional qualifications for telehealth and mHealth professionals at EU level? (in terms of efficiency, societal costs, etc.)</p>
Other issues (A6)	<p>What are the existing or future (planned) national rules on the provision of services by online pharmacies and their potential impact on the cross-border provision and circulation of these services and products?</p> <p>What measures that should be taken at EU level in order to counteract these obstacles concerning existing or future (planned) national rules on the provision of services by online pharmacies and their potential impact on the cross-border provision and circulation of these services and products?</p> <p>What are the costs and benefits of removing cross-border obstacles to the free movement regarding the online sales of pharmaceuticals between Member States? (in terms of efficiency, societal costs, etc.)</p>

8.1.2 Artificial intelligence in healthcare

Table 57. Artificial intelligence in healthcare initial research questions

Area	Research questions (RQ)
AI in healthcare (A7)	What are the existing or future (planned) national rules regulating the adoption and use of AI in healthcare ? (covering legislation, standardisation measures, guidelines, codes of conduct etc.)?
	To what extent the existing or future (planned) national rules mapped take into account the Ethics guidelines for trustworthy Artificial Intelligence of the High-level group (and any future horizontal initiative on AI at the EU level building on this work)?
	What are the existing or future (planned) national rules and practices (incl. guidelines, codes of conduct etc.) concerning standards used for AI in healthcare ?
	What are the existing or future (planned) national rules and practices concerning medical data gathering, organisation and use of medical data for developing AI in healthcare ?
	From a legal perspective, what is the taxonomy/classification of AI use in healthcare that could have distinct legal implications in terms of safety and liability?
Needs of healthcare sector and interaction with AI (A8)	What are the implications of AI for the medical profession and the needs of healthcare providers and professionals, per category (doctors, nurses, hospital administrators, other categories) of using AI applications?
	Which types of applications are most relevant for each target group?
	What are the needs for using AI for research purposes in healthcare? (national examples, best practices and emerging needs)
	What are the needs (including, but not only, in relation to medical data) of researchers, engineers, start-ups, companies in developing AI for healthcare?
	What are the current take up levels and impact of AI solutions by type of healthcare providers (primary, secondary, tertiary care) and of advantages and disadvantages of using AI solutions? (taking into account more advanced and less advanced Member States).
	What is the potential extent of scale up of AI solutions from research to healthcare services?
	What are the distinct elements (specificities) that differentiate the deployment of AI in healthcare compared to other domains in terms of liability?
Liability questions / elements to be considered (A9)	To what extent is the conventional distinction between products and services being affected by the incorporation of AI into healthcare?
	To what extent are the liability rules applicable to products (strict product liability) and to services (negligence) impacted by the deployment of AI in healthcare? Should the current legal tests and dichotomies change?
	What is the impact of these regulations on a possible new specific regulation on AI liability in healthcare, considering that the healthcare sector is heavily regulated (e.g., Medical Devices Regulations (MDR), Pharmaceuticals, regulated medical profession)?
	What are the distinct policy/legal considerations in healthcare that need to be taken into account compared to other sectors ?
	Should a lex specialist provisions/derogations be introduced to accommodate the specificities on AI in healthcare? How should gaps require to be filled by a new AI liability framework?
	Are product liability rules concerning manufacturing defects, design defects and warning defects being impacted by the emergence of AI systems in medicine?
	Should AI generated medical information intended for use by healthcare professionals or patients be regulated? Should such information be regulated as a product? As a service? Or on some other way, if so, how?
	To what extent the existing or future (planned) national rules on the organisation and provision of healthcare allow or prohibit that healthcare services (e.g., diagnosis, surgical interventions executed by autonomous robots, etc.) are provided by fully autonomous AI-based healthcare applications/systems without any involvement of a healthcare professional?
	In cases where healthcare services provided by fully autonomous AI-based solutions are allowed by the national law, it should be assessed whether supervision by a healthcare professional is or is not required.
	What is the economic and behavioural (i.e., trust and acceptance of AI) impact in terms of AI liability options that would be legally-sound and provide the most benefits to the patient (medical costs and best treatment) and to hospitals and physicians (workload, costs to healthcare providers, insurances, etc.)?

Area	Research questions (RQ)
	<p>What is the economic impact of different liability options on the costs of treatment involving AI systems?</p> <p>What is the economic and behavioural impact of different options on the physicians'/hospitals' willingness to use or not AI technologies?</p> <p>What is the economic impact of different options on the existing systems of healthcare insurance systems?</p> <p>What is the economic impact of different liability options on adding to the costs of using AI systems for diagnostic, treatment or management purposes?</p> <p>What is the economic impact of liability options on the manufacturers of AI medical systems?</p> <p>What is the economic impact of different liability frameworks on the economic viability of AI medical systems?</p> <p>What is the economic impact of options on the patients' needs in connection to medical costs?</p> <p>What is the impact on trust by patients and citizens on different options in embracing AI technologies in healthcare?</p> <p>What are the existing or future (planned) national liability rules on the organisation and provision of healthcare that can concern the liability of AI developers and all the other actors using and benefiting from AI-based services and products when used in healthcare sector, with and without the supervision of a healthcare professional/provider?</p> <p>What is the impact of different national rules on the functioning of the internal market?</p> <p>What are the existing or future (planned) national rules on the organisation and provision of healthcare that can concern the liability for fully autonomous AI-based solutions when used in the healthcare sector?</p> <p>What is the impact of national rules on the functioning of the internal market?</p> <p>What are the existing or future (planned) national rules defining who should be considered a "health professional", and more specifically, whether this definition covers actions by fully autonomous AI healthcare applications/systems without any involvement of a human healthcare professional?</p> <p>What is the impact of different national rules on the functioning of the internal market?</p> <p>What are the existing or future (planned) national rules of liability and malpractice and if they differ between fully autonomous AI systems and healthcare professionals, as well as the impact on possible different standards applied to the healthcare professionals?</p> <p>What is the impact of different national rules on the functioning of the internal market?</p> <p>What are the existing or future (planned) national rules on the minimum standards of diligence that would be required from the AI producers or deployers with regard to the AI applied in healthcare for example for the purposes of establishing liability (for example, the "lege artis" standards frequently applied to healthcare provided by a healthcare professional may not be applicable to healthcare services provided by AI-based solutions)</p> <p>What are the rules and practices adopted at EU and national level for algorithms that evolve through continuous learning and for update deployment in AI-based solutions, and health sector-specific rules related to liability in such cases.</p>
Approval, certification, authorisation, reimbursement of AI in healthcare (A10)	<p>What are the existing or future (planned) rules adopted at the EU and national level on the conditions under which AI-based products are approved, certificated, authorised or reimbursed in one Member States and to what extent these products can be used under the same conditions in another Member States?</p> <p>What is the impact of different national rules on the functioning of the internal market?</p> <p>What are the existing or future (planned) rules adopted at the EU and national level concerning the exchange of information/good practices between notified bodies or medicine agencies concerning the conditions under which AI-based products are approved in different Member States?</p> <p>What is the impact of different national rules on the functioning of the internal market?</p> <p>What are the existing or future (planned) rules and practices adopted at EU and national level for algorithms that evolve through continuous learning and for upgrades and modifications rules for certification and re-certification (by notified bodies, medicine agencies or other authorities)?</p> <p>What is the impact of different national rules on the functioning of the internal market?</p> <p>What are the existing or future (planned) national rules describing how regulators can access algorithms, when used in healthcare, and how algorithms must be able to self-explain a dynamic</p>

Area	Research questions (RQ)
AI and benchmarking (A11)	approval and follow-up framework might be especially necessary when looking at self-learning algorithms?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) national and EU level practices on the regulatory assessment of self-learning algorithms when used in healthcare and of upgrade deployment of AI-based solutions?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules and practices at EU and national level that support medical decisions or are involved in areas related to health (including well-being; etc.), but are not covered by the Medical Devices Regulation and are not accredited by the notified bodies or medicine agencies?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules and common approaches adopted at the EU and national level on the transparency of AI-based systems when used in healthcare, including any obligation to record and store data?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules and common approaches adopted at the EU and national level concerning the transparency of algorithms. Rules and common approaches adopted at the EU and national level concerning the possibility of providing cross-border healthcare services/ products relevant for healthcare involving an AI component?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules and practices adopted at EU and national level and supporting regulators (notified bodies, medicines agencies, etc.) in evaluating AI health applications (information about input data and definitions, information about input datasets, existence of control data sets on which data are tested, approval rules, rules for re- approval in case of evolution of the algorithm, etc.)?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules concerning governance structures managing the access and testing of AI applications in clinical settings and their inclusion in registries or other databases, and the support provided to regulators (notified bodies or medicine agencies)?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules at national and international level concerning the benchmarking of the quality of AI-based systems in healthcare?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules at national and international level concerning quality criteria for AI in healthcare , with examples on different domains?
	What is the impact of different national rules on the functioning of the internal market?
	What are the existing or future (planned) rules at national and international level concerning the creation and/or the functioning of test centres for AI in healthcare , with examples on different domains?
	What is the impact of different national rules on the functioning of the internal market?

Source: Authors' elaboration based on the Technical Specifications

8.1.3 Governing the use of health data

Table 58. Governing the use of health data initial research questions

Area	Research questions (RQ)
Use of health data for healthcare, research and policy marking (A12)	What are the costs and benefits of not implementing interoperability and not sharing health data not only for direct provision of healthcare, but also for research and policy making?
	What are the costs and benefits of setting up (or not) national data governance structures, and potentially such structures at the EU level in terms of efficiency, societal benefits of increased reuse of health data, etc.? (analysis based on the information collected in the SANTE project titled ' <i>Assessment of the Member States' rules on health data in the light of GDPR 2019/2020</i> ')
Access of policy makers, regulators to health data (A13)	What are the costs and benefit for access (or not) of policy makers and regulators to health data planning, management, administration and improvement of the health and care systems; protection against serious cross-border threats to health; ensuring safety of medicines and medical devices?
Sharing / access to data (A14)	What are the costs and benefit for access (or not) of health data between businesses, between business and government (and viceversa), at national level and between Member States?
Citizens' control over their own health data (A15)	What are the costs and benefit concerning citizens accessing (or not) their own data and ensuring the portability of health data between different healthcare providers and between different Member States?
	What are the costs and benefit concerning citizens accessing (or not) their own data and ensuring the portability of health data between their m-health devices, EHRs and healthcare providers?
	What are the costs and benefits concerning citizens controlling the storage of their health data in their EHR, including m-health data?

Source: Authors' elaboration based on the Technical Specifications

8.1.4 Evaluation of Article 14 of Directive 2011/24/EU

Table 59. Evaluation of Article 14 of Directive 2011/24/EU initial research questions

Area	Research questions
Application of Art. 14 and accompanying acts (A16)	What has been the impact of Article 14 of the Directive 2011/24/EU on cross-border healthcare/patient mobility ?
	What has been the impact of Article 14 of the Directive 2011/24/EU on the use of medical information for the provision of healthcare, but also for public health and research?
	What has been the impact of Article 14 of the Directive 2011/24/EU on the provision of digital health services and products, including telemedicine (and its reimbursement)?
	What has been the impact of Article 14 of the Directive 2011/24/EU on national healthcare systems ?
	What was the impact of article 14 on the access of patients to their electronic health records?
	What was the impact of article 14 on the interoperability of electronic health records and e-prescriptions?
Effectiveness (A17)	To what extent were the objectives reached, as they were set out in Article 14 (2) of the Directive ?
	What were the qualitative and quantitative effects of the eHealth Network on the cooperation and exchange of information between Member States? How were these effects achieved?
	To what extent can they be attributed to the eHealth Network, e-Prescriptions and Patient Summaries, European Electronic Health Record exchange format , etc.? To what extent can be attributed to eHealth Network the interoperability of e_prescriptions and electronic health records?
	To what extent was the eHealth Network effective in supporting patients having access to their health data? (patients who have received treatment are entitled to a written or electronic medical record of such treatment, and access to at least a copy of this record)
	How effective was the eHealth Network in uptake of interoperability standards in health area?
	How effective was the setting up of the eHealth Digital Service Infrastructure in stimulating interoperability and cross-border exchange of health data?
	To what extent was the intervention of the eHealth Network effective in stimulating the use of health data for research and policy making ?

Area	Research questions
	<p>To what extent was the intervention of the eHealth Network effective in stimulating the primary and secondary use of health data?</p> <p>To what extent was the eHealth Network effective in supporting the use of health data for medical diagnosis and treatment, public health (including planning, provision of healthcare, management of health or social care systems and services, regulatory purposes, approval of medical devices, protecting against cross-border health threats, provision of telemedicine, tele-health, m-health) and for scientific or historical research and innovation?</p> <p>What were the factors that influenced the observed achievements and to what extent?</p> <p>Which factors hindered the attainment of the objectives and to what extent? How do these factors link to the actions carried out under Article 14? To what extent were there external factors that influenced the results?</p>
Efficiency (A18)	<p>To what extent have the actions carried out under Article 14 been realised in a cost-effective way, including eHDSI/MyHealth@EU?</p> <p>Looking closely at both the costs and benefits of Article 14 as they accrue to different eHealth stakeholders, how efficient has the implementation of Article 14 been for each type of stakeholder (citizens, patients, healthcare professionals, policy makers, researchers, companies (pharmaceutical sector, AI) etc.)?</p> <p>To what extent are the costs justified and proportionate given the effects observed/objectives achieved/ benefits obtained in general? How proportionately were the costs of the intervention borne by different stakeholder groups taking into account the distribution of the associated benefits?</p> <p>If there are significant differences in costs (or benefits) between Member States, what is causing them? How do these differences link to the intervention?</p> <p>What factors influenced the efficient functioning of the intervention and to what extent? What factors hindered it and to what extent? What is the connection between these factors and the actions laid out in Article 14?</p> <p>Which factors influenced the cost side and which ones influenced the benefit side? To what extent? To what extent were these factors linked to the intervention described in Art. 14? To what extent were there external factors that influenced the results?</p>
Relevance (A19)	<p>To what extent are the objectives and provisions of Article 14 still relevant, considering current needs and how they have evolved since the adoption of the Directive?</p> <p>How relevant is article 14 to EU citizens? How did the article contribute to supporting citizens to access their own health data and ensure portability of these data?</p> <p>How relevant is the article 14 for interoperability of electronic health records and e-Prescriptions?</p> <p>How relevant is the article 14 for the provision of digital health services, including tele-medicine, tele-health, tele-monitoring?</p> <p>How relevant is the article 14 for the secondary use of health data (use of data for research, policy making and regulatory purposes)?</p> <p>How relevant is the article 14 for the uptake of interoperability standards in health rea?</p> <p>To what extent the provision of article 14 are relevant for the secondary use of health data (for policy making, regulatory purposes, research and innovation)?</p> <p>To what extent have the original objectives proven to be appropriate to facilitate the cooperation and exchange of information between Member States?</p> <p>How well adapted is Article 14 to subsequent technological or scientific advances (e.g. the use of Big Data and Artificial Intelligence in the field of healthcare)?</p> <p>To what extent does Article 14 facilitate both the processing of health data for treatment (e.g. through the eHealth Digital Service Infrastructure and the National Contact Points for eHealth), and further compatible processing of health data for research and policy-making?</p>
Coherence (A20)	<p>To what extent are the provisions of Article 14 coherent with wider EU policy and with the European Health Data Space (especially the use of data for medical diagnosis, public health (including planning, provision of healthcare, management of health or social care systems and services, regulatory purposes, approval of medical devices, protecting against cross-border health threats) and for scientific or historical research and innovation)?</p> <p>To what extent the provisions of article 14 are coherent with new development in secondary use of health data, such as the appearance of data permit authorities?</p> <p>To what extent is the cooperation described in art. 14 coherent with other Networks/cooperation possibilities which have similar objectives (especially for the use of data for policy making, research and innovation – eg Findata, French Data Hub etc)?</p>

Area	Research questions
	<p>To what extent is Article 14 coherent with international obligations?</p> <p>To what extent is the eHealth Network coherent internally (e.g. there is coherence between its actions/activities/tasks)?</p> <p>To what extent is the eHealth Network able to implement the European Health Data Space in its entirety, as requested by the mission letter of Commissioner Kyriakides?</p> <p>To what extent can article 14 and the eHealth Network ensure that citizens have control over their own personal health data?</p>
EU added value (A21)	<p>What is the added value produced by the provisions of Article 14, compared to what could reasonably have been expected from the Member States acting in the absence of the network at national or regional level?</p> <p>What would be the most likely consequences of stopping the eHealth Network/ repealing Art. 14?</p> <p>How should the eHealth Network and article 14 be modified to increase their impact on interoperability of electronic health records, e-Prescriptions and health data, in general?</p> <p>How should the eHealth Network and article 14 be modified to increase the use of data for research, policy making and regulatory purposes?</p> <p>How should the article 14 be modified in order to increase the cross-border provision of digital health services, including telemedicine, tele-health, m-health?</p> <p>How should the eHealth Network and article 14 be modified to increase their impact, especially in the light of new technological developments and the use of data, including for scientific research, policy making, reporting, protecting against cross-border health threats etc.?</p> <p>How should the tasks of the eHealth Network and article 14 be modified to increase their impact, especially in relation to setting up the European Health Data Space, ensuring the control of citizens over their own personal health data and the use of data for medical diagnosis, public health (including planning, provision of healthcare, management of health or social care systems and services, regulatory purposes, approval of medical devices, protecting against cross-border health threats) and for scientific or historical research and innovation?</p> <p>What kind of cooperation at EU level would be most adequate for ensuring an adequate coordination of national efforts in the context of the European Health Data Space (especially to ensure access of citizens to their own health data, but also access to data for healthcare, research and policy making)?</p> <p>What kind of cooperation at EU level would be most adequate for ensuring an adequate coordination of national efforts in the context of the European Health Data Space (especially to ensure secondary use of health data and provision of digital health services)?</p>

Source: Authors' elaboration based on the Technical Specifications

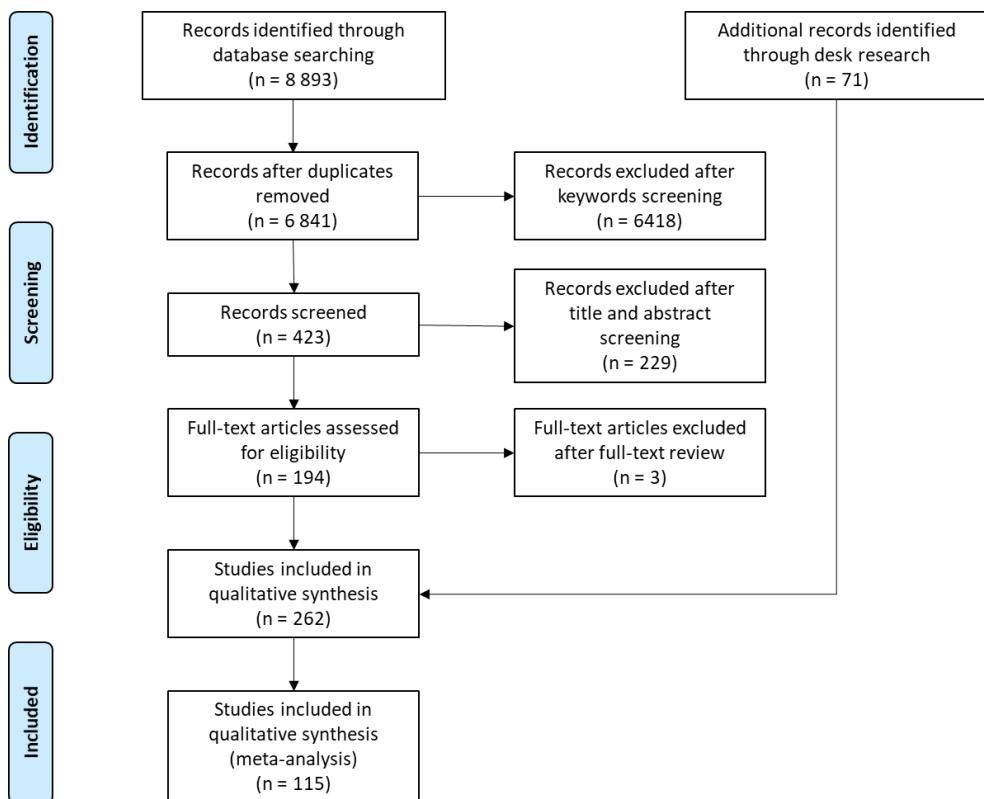
8.2 Search strings and PRISMA diagrams

8.2.1 Digital health products and services

Table 60. Digital health products and services search strings

Area	Search string	Source	Results
Definitions (A1)	(eHealth OR telemedicine OR telehealth) AND ((legal) OR (regulations) OR (governance)) AND (healthcare) AND (EU OR Europe OR Member States OR Canada OR United States)	PubMed	1,065
	TOPIC: (eHealth definitions) OR TOPIC: (telemedicine definitions) OR TOPIC: (telehealth definitions) OR TOPIC: (mHealth definitions) AND TOPIC: (national rules) AND TOPIC: (Europe) OR TOPIC: (member states)	ISI Web of Science	2,092
Approval, certification, authorisation and reimbursement rules that can impact on free movement of digital health services and products (A2)	((digital health) OR (eHealth) OR (Telehealth) OR (telemedicine) OR (mHealth) OR (mobile health)) AND ((approval) OR (certification) OR (authorisation) OR (reimbursement))	PubMed	913
	TOPIC: (eHealth certifications) OR TOPIC: (eHealth authorisation) OR TOPIC: (eHealth reimbursement) OR TOPIC: (multi-party medical consultations) OR TOPIC: (HTA) AND TOPIC: (Laws) OR TOPIC: (regulations) AND TOPIC: (Europe)	ISI Web of Science	742
Interoperability between mHealth, telehealth and electronic health records/registries, and interoperability with other IoT (A3)	(eHealth OR electronic health records OR EHR) AND (data sharing OR interoperability OR cross-border) AND (legal OR regulations OR advantages OR patient rights)	PubMed	536
	TOPIC: (health data interoperability) AND TOPIC: (costs and benefits of interoperability) OR TOPIC: (data transfer costs and benefits) OR TOPIC: (mobile applications) AND TOPIC: (national rules) OR TOPIC: (national laws) AND TOPIC: (Europe)	ISI Web of Science	623
Privacy and liability rules in relation to eHealth services and products (A4)	((eHealth) OR (telemedicine) OR (telehealth)) AND ((security) OR (threats) OR (privacy) OR (digital authentication)) AND (regulations)	Pubmed	485
	(eHealth) AND TOPIC: (safety and liability) OR TOPIC: (digital authentication for patients) OR TOPIC: (digital authentication for doctors) OR TOPIC: (privacy and data protection) AND TOPIC: (national rules) OR TOPIC: (national laws) AND TOPIC: (Europe)	ISI Web of Science	484
Professional qualifications for providing telehealth services (A5)	((eHealth) OR (telemedicine)) AND ((cross-border) OR (professional qualification) OR (certification) OR (license))	Pubmed	315
	TOPIC: (telehealth services) OR TOPIC: (eHealth services or products) AND TOPIC: (telehealth professional qualifications) OR TOPIC: (telehealth professional training) OR TOPIC: (telehealth provider qualifications) AND TOPIC: (national rules) OR TOPIC: (national laws) AND TOPIC: (Europe)	ISI Web of Science	663
Other issues (A6)	(telepharmacy OR online pharmacy OR e-Pharmacy) AND (regulation OR laws OR national rules)	Pubmed	359
	TOPIC: (online pharmacies) OR TOPIC: (telepharmacy) AND TOPIC: (national rules) OR TOPIC: (national laws) AND TOPIC: (Europe)	ISI Web of Science	616

Source: Authors' elaboration

Figure 19. Digital health products and services PRISMA diagram

Source: Authors' elaboration

8.2.2 Artificial intelligence in healthcare

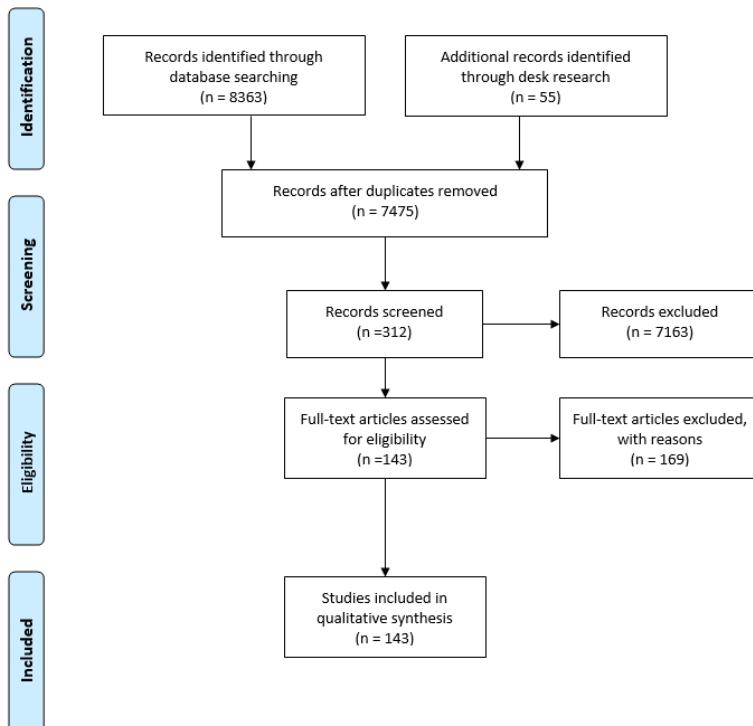
Table 61. Artificial intelligence in healthcare search strings

Topic	Search string	Source	Records
AI in Healthcare	(Artificial intelligence) AND ((legal) OR (regulations) OR (governance)) AND (healthcare)	Pubmed	314
	TOPIC: (artificial intelligence) OR TOPIC: (AI) AND TOPIC: (healthcare) AND TOPIC: (ethics national laws) OR TOPIC: (data national laws) OR TOPIC: (trustworthy AI laws) AND TOPIC: (Europe)	ISI WoS	645
Needs of healthcare sector and interaction with AI (applications and take up levels)	Artificial Intelligence AND healthcare AND ((societal impact) OR (ethics) OR (medical professional) OR (researchers))	Pubmed	857
	TOPIC: (artificial intelligence in healthcare) OR TOPIC: (AI in healthcare) OR TOPIC: (challenges for companies and researchers) OR TOPIC: (national applications and best practices) OR TOPIC: (impact healthcare professions) OR TOPIC: (medical professionals) AND TOPIC: (Europe) AND TOPIC: (national level)	ISI WoS	844
Liability questions / elements to be considered	artificial intelligence AND ((malpractice claim) OR (economy) OR (private sector) OR (legal liability) OR (accountability))	Pubmed	1270
	TOPIC: (artificial intelligence liability) OR TOPIC: (artificial intelligence malpractice) OR TOPIC: (artificial intelligence trust and acceptance)	ISI WoS	149
Approval, certification, authorisation, reimbursement of AI in healthcare	artificial intelligence AND (cross-border OR reimbursement OR certification OR requirements OR regulations) AND healthcare – 719 records found.	Pubmed	719
	TOPIC: (AI) AND TOPIC: (healthcare) OR TOPIC: (artificial intelligence) AND TOPIC: (cross-border healthcare) OR TOPIC: (testing AI) AND TOPIC: (Laws)	ISI WoS	547

Topic	Search string	Source	Records
AI and benchmarking	(Artificial Intelligence OR AI) AND (healthcare) AND (benchmarking OR testing OR evaluation OR assessment) AND (regulation OR legal OR impact)	Pubmed	1372
	TOPIC: (artificial intelligence benchmarking) OR TOPIC: (artificial intelligence evaluation) OR TOPIC: (artificial intelligence assessment) AND TOPIC: (healthcare)	ISI WoS	1619

Source: Authors' elaboration

Figure 20. Artificial intelligence in healthcare PRISMA diagram



Source: Authors' elaboration

8.2.3 Governing the use of health data

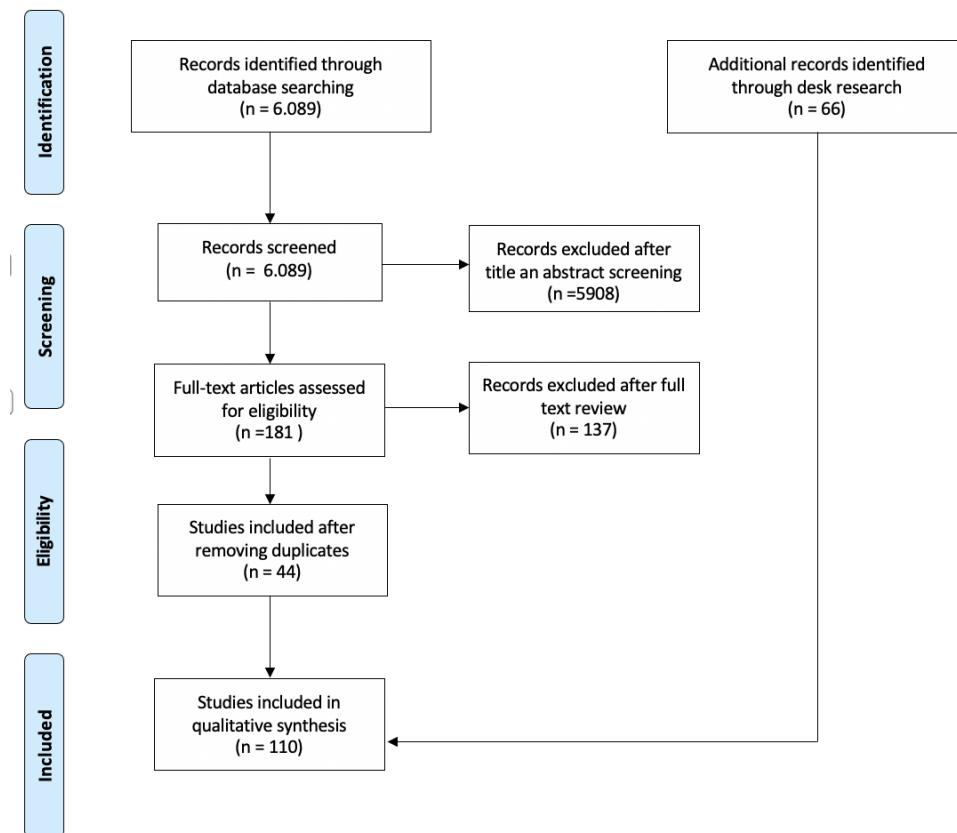
Table 62. Governing the use of health data search strings

Area	Search string	Source	Results
Use of health data for healthcare, research and policy marking (A12) (C1)	(EHR OR electronic health records OR eHealth data) AND (access or sharing) AND (government OR research OR governance OR policy makers) AND (health) AND (cross border OR member states or rules or regulations)	PubMed	990
	(ehealth data governance) AND TOPIC: (interoperability) OR TOPIC: (cross border) AND TOPIC: (costs and benefits) OR TOPIC: (economic impact) AND TOPIC: (laws) OR TOPIC: (national rules) AND TOPIC: (Europe)	ISI Web of Science	1,188
Access of policy makers, regulators to health data (C2)	(health data) AND (data sharing) AND ((government) OR (member states)) AND (costs OR benefits)	Pubmed	516
	TOPIC: (government access) OR TOPIC: (eHealth data access) OR TOPIC: (electronic health records OR EHR) AND TOPIC: (costs and benefits)	ISI Web of Science	726
Sharing / access to data (C3)	(health data) AND (data sharing OR data access) AND (private sector OR government OR member states) AND (costs OR benefits) AND (EU OR Europe OR united states OR Canada)	Pubmed	1,217

Area	Search string	Source	Results
Citizens' control over their own health data (C4)	TOPIC: (ehealth data access) OR TOPIC: (health data access) OR TOPIC: (electronic health records access) AND TOPIC: (government OR business OR private sector) AND TOPIC: (costs and benefits)	ISI Web of Science	958
	(electronic health records OR health data) AND (patient rights OR citizens) AND (benefits OR costs) AND access	Pubmed	323
	TOPIC: (electronic health records) AND TOPIC: (health data) AND TOPIC: (patient rights) AND TOPIC: (costs OR benefits)	ISI Web of Science	171

Source: Authors' elaboration

Figure 21. Governing the use of health data PRISMA diagram



Source: Authors' elaboration

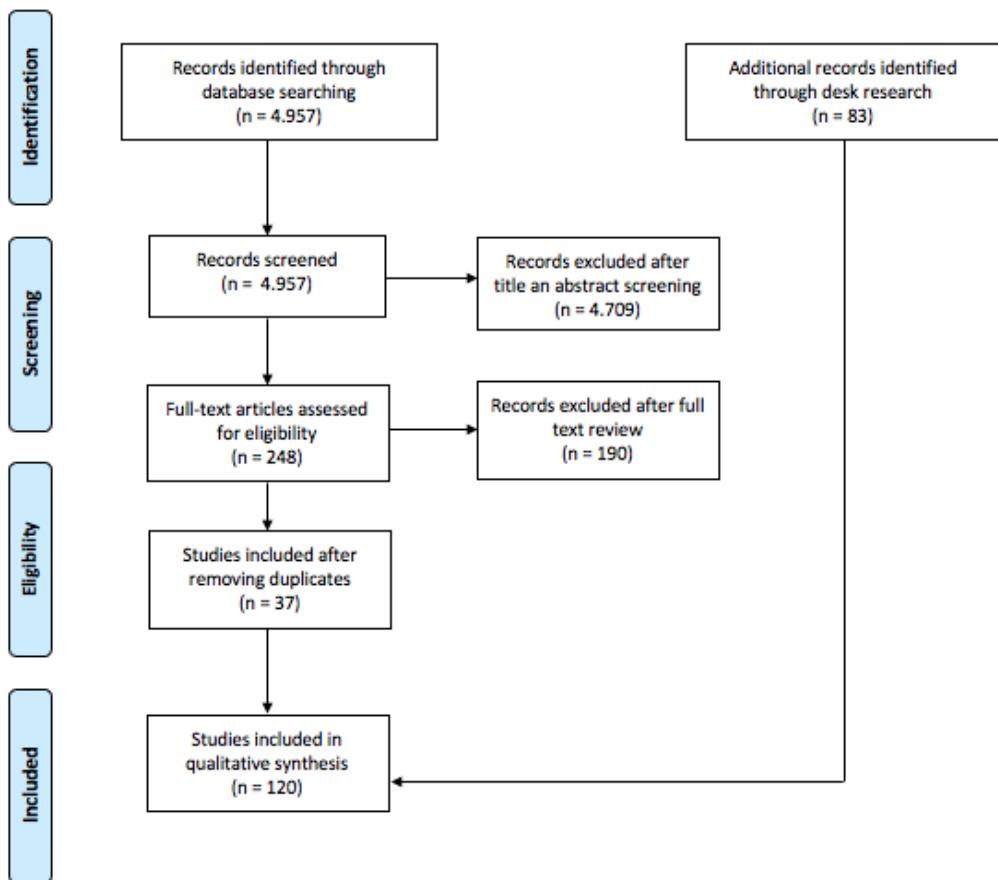
8.2.4 Evaluation of Article 14 of Directive 2011/24/EU

Table 63. Evaluation of Article 14 of Directive 2011/24/EU search strings

Lot 4 (L4) area	Search string	Source	Results
Application of Art. 14 and accompanying acts (D1)	(Directive 2011/24 OR cross border) AND (patient mobility OR products OR healthcare) AND (impact OR application)	PubMed	163
	TOPIC: (Directive 2011/24/EU) OR TOPIC: (cross-border healthcare) AND TOPIC: (patient rights) AND TOPIC: (patient mobility) OR TOPIC: (use of medical information) OR TOPIC: (digital health services and products) OR TOPIC: (national healthcare systems)	ISI Web of Science	1,545
Effectiveness (D2)	((Directive 2011/24) OR (cross border)) AND (effectiveness) AND (Europe OR EU)	PubMed	103
	TOPIC: (Directive 2011/24/EU) OR TOPIC: (cross-border healthcare) OR TOPIC: (patient mobility) AND TOPIC: (effectiveness)	ISI Web of Science	427
Efficiency (D3)	(cross border OR Directive 2011/24/EU) AND (cost OR benefit OR finance OR fund OR insurance OR efficiency) AND (EU or Europe OR member states)	PubMed	125
	TOPIC: (Directive 2011/24/EU) OR TOPIC: (cross-border healthcare) OR TOPIC: (patient mobility cost) AND TOPIC: (effectiveness) OR TOPIC: (insurance) AND TOPIC: (Directive 2011/24/EU cost)	ISI Web of Science	367
Relevance (D4)	(cross border) AND (healthcare) AND ((big data) OR (eHealth) OR (data) OR (portability) OR (relevance) OR (NCP) OR (patients)) AND ((EU) or (Europe) OR (member states))	PubMed	125
	TOPIC: (Directive 2011/24/EU) OR TOPIC: (cross-border healthcare) AND TOPIC: (relevance) OR TOPIC: (NCP) OR TOPIC: (patients) AND TOPIC: (EU OR member states OR Europe)	ISI Web of Science	619
Coherence (D5)	(cross border) AND (healthcare) AND ((eHealth) OR (coherence) OR (personal data) OR (cooperation) OR (data space) OR (patients) OR (policy)) AND ((EU) or (Europe) OR (member states))	PubMed	134
	TOPIC: (Directive 2011/24/EU) OR TOPIC: (cross-border healthcare) OR TOPIC: (eHealth) AND TOPIC: (coherence) OR TOPIC: (data cooperation) AND TOPIC: (EU OR member states OR Europe)	ISI Web of Science	794
EU Added Value (D6)	(cross border) AND (healthcare) AND (added value OR patients OR health data OR tasks) AND (EU OR Europe OR member states)	PubMed	119
	TOPIC: (Directive 2011/24/EU) OR TOPIC: (cross-border healthcare) OR TOPIC: (eHealth) AND TOPIC: (added value) OR TOPIC: (cross-border healthcare implementation) AND TOPIC: (EU OR member states OR Europe)	ISI Web of Science	436

Source: Authors' elaboration

Figure 22. Evaluation of Article 14 of Directive 2011/24/EU PRISMA diagram



Source: Authors' elaboration

8.3 Overview of the consultation phase

8.3.1 In-depth interviews

Digital health products and services in-depth interviews

Stakeholder category	Interviewer	Main focus topics
European organisation on mHealth	EY	Interoperability Authorisation, certification, reimbursement (mHealth legal framework)
eHealth expert	EY	Authorisation, certification, reimbursement Interoperability (ePrescription)
Member State representative (Ministry of Health)	EY – Open Evidence	Interoperability Safety and liability
Patient organisation	EY – Open Evidence	Liability, safety and security
Member State (eHealth agency)	EY	Interoperability Authorisation, certification, reimbursement (Telemedicine framework)
Representatives from MedTech industry	EY – Open Evidence	Approval, certification, reimbursement of eHealth services and products Liability rules for eHealth services and products, professional qualifications recognition Online pharmacies Primary/secondary use of health data
Representatives from MedTech industry	EY	Authorisation, certification Interoperability

Artificial intelligence in healthcare in-depth interviews

Stakeholder category	Interviewer	Main focus topics
Medical director – health care professionals	UPM	Behavioural Impact interview: perspective from medical professional background <ul style="list-style-type: none"> • Liability of AI in healthcare • Needs of healthcare sector and interaction with AI. • AI impact on behaviour • Economic impact • Liability of AI in healthcare
Patients' association	UPM – Open Evidence	Behavioural Impact interview: perspective from patient associations <ul style="list-style-type: none"> • Consumer Trust in AI systems • Implications of using medical information and autonomous systems. • Economic impact • Liability of AI in healthcare
Representative of medical informatics professional association	UPM	Behavioural Impact interview: perspective from professionals <ul style="list-style-type: none"> • Black box medicine and questions of liability. • Behavioural impact of AI liability options.
Law scholar	UPM	Future regulation of AI in the healthcare sector <ul style="list-style-type: none"> • Legal implications • Safety and liability • Future regulation / elements to be considered • Economic impact
HTA scholar	UPM – Open Evidence	<ul style="list-style-type: none"> • AI services in healthcare • Assessment and labelling • Health data sharing / access • Costs and benefits

Stakeholder category	Interviewer	Main focus topics
Industry representative	UPM	<p>Industry perspective of AI use in the healthcare sector</p> <ul style="list-style-type: none"> • AI in healthcare: expectations, needs and implications. • Liability • Economic impact

Governing the use of health data in-depth interviews

Stakeholder category	Interviewer	Main focus topics
Pharmaceutical company	Open Evidence	<p>Sharing health data between B2G and G2B</p> <p>Citizen control over health data</p>
Industry representative	Open Evidence	Sharing health data for research and innovation
High-Level Expert Group on Business to Government Data Sharing	Open Evidence	Sharing health data for research and innovation
Innovation institution	Open Evidence	Sharing health data for healthcare provision cross-border and for research and innovation
Health data authority	Open Evidence	Sharing health data for research and innovation
Researcher	Open Evidence	Sharing health data for research and innovation
Health Authority	Open Evidence	Sharing health data for healthcare provision, research and innovation
Scholar	Open Evidence	<p>Patient portability of health data</p> <p>Sharing health data for healthcare provision, research and innovation</p>
Medicine and Device Agency	Open Evidence	Access of health data for regulating and policy making.

Evaluation of Article 14 of Directive 2011/24/EU in-depth interviews

Stakeholder category	Interviewer	Main focus topics
Member State representative (Ministry of Health)	Open Evidence	<ul style="list-style-type: none"> • Application of Art. 14 and accompanying acts • Effectiveness • Efficiency
SITRA, THEDAS Action Joint	Open Evidence	<ul style="list-style-type: none"> • Application of Art. 14 and accompanying acts • Effectiveness • Efficiency • Coherence
Former member of the eHealth Network	Open Evidence	<ul style="list-style-type: none"> • Application of Art. 14 and accompanying acts • Effectiveness • Efficiency
Industry representative	Open Evidence	<ul style="list-style-type: none"> • Application of Art. 14 and accompanying acts • Effectiveness • Efficiency
Industry representative	Open Evidence	<ul style="list-style-type: none"> • Application of Art. 14 and accompanying acts • Effectiveness • Efficiency
Patients' association	Open Evidence	<ul style="list-style-type: none"> • Application of Art. 14 and accompanying acts • Effectiveness • Efficiency

8.3.2 Workshops

Digital health products and services workshops

Workshop 1 – European digital healthcare framework	
Date	25/01/2021
Area	European digital healthcare framework
Objective	Understand the challenges, issues, impacts and benefits of a European regulation and harmonization of the digital healthcare framework.
Main RQs addressed	<ul style="list-style-type: none"> • A2 – Certification • A4 – Privacy and liability • A5 – Professionals qualifications
Participants	<p>Panel of six eHealth experts:</p> <ul style="list-style-type: none"> • eHealth organisations, • Representatives of healthcare professionals, • Representatives of MedTech industry.
Moderator (s)	EY

Workshop 2 – European digital healthcare framework	
Date	17/02/2021
Area	European digital healthcare framework
Objective	Understand the challenges, issues, impacts and benefits of a European regulation and harmonization of the digital healthcare framework, especially on mobile health applications.
Main RQs addressed	<ul style="list-style-type: none"> • A2 – Labelling and reimbursement • A4 – Privacy and liability • A5 – Professionals qualifications
Participants	<p>Panel of five eHealth experts from:</p> <ul style="list-style-type: none"> • Independent eHealth experts, • Representatives of healthcare professionals, • Representatives of MedTech industry, • HTA organisations.
Moderator (s)	EY

Artificial intelligence in healthcare workshops

Workshop 1. AI Liability in health – US and legal perspective	
Date	27/01/2021
Area	AI Liability in health – US and legal perspective
Objective	To gather experts' opinions on legal questions regarding liability frameworks applicable to AI systems used in healthcare. The experts' consultation will help to fill knowledge gaps as identified in the literature.
Main RQs addressed	<ul style="list-style-type: none"> 1. Overview of AI uses in healthcare. 2. Manufacturer's liability for three types of defects <ul style="list-style-type: none"> • Design defects • Warning defects • Manufacturing defects 3. Causation 4. Burden of proof on plaintiff 5. Relationship between physicians and AI manufacturers for continuously learning AI 6. Learned intermediaries, experts in the field and consumer advertising. 7. (Unavoidable unsafe products)
Participants	Participants 5 <ul style="list-style-type: none"> • Legal scholars • Computer science scholars
Moderator	Open Evidence

Workshop 2. AI Liability in health – practitioners' perspective	
Date	03/02/2021
Area	AI Liability in health – practitioners' perspective
Objective	To gather experts' opinions on legal questions regarding liability frameworks applicable to AI systems used in healthcare. The experts' consultation will help to fill knowledge gaps as identified in the literature.
Main RQs addressed	<ul style="list-style-type: none"> 1. Overview of AI uses in healthcare 2. Manufacturer's liability for three types of defects <ul style="list-style-type: none"> • Design defects • Warning defects • Manufacturing defects 3. Causation 4. Burden of proof on plaintiff 5. Relationship between physicians and AI manufacturers for continuously learning AI 6. Learned intermediaries, experts in the field and consumer advertising 7. (Unavoidable unsafe products)
Participants	Participants 7 <ul style="list-style-type: none"> • HTA experts • Biomedical engineering • Medical doctors • Industry representative
Moderator	Open Evidence

Governing the use of health data workshops

Workshop 1. Access and use of health data for primary and secondary purposes	
Date	12/02/2021
Area	Costs and benefits of primary use of health data, costs and benefits of access to health data for secondary purposes, and citizen access to health data
Objective	Fill the gaps identified in the gap analysis
Main RQs addressed	<ul style="list-style-type: none"> • A12 Use of health data for healthcare, research and policy marking • A13 Access of policy makers, regulators to health data • A14 Sharing / access to data • A15 Citizens' control over their own health data
Participants	<p>Panel of five eHealth experts from:</p> <ul style="list-style-type: none"> • Independent eHealth and citizen health data experts, • Representatives of independent European bodies • Representatives of MedTech industry,
Moderator	Open Evidence

Workshop 2. Primary and Secondary Use of Health Data	
Date	15/02/2021
Area	Costs and benefits of primary use of health data, costs and benefits of access to health data for secondary purposes, and citizen access to health data
Objective	Fill the gaps identified in the gap analysis
Main RQs addressed	<ul style="list-style-type: none"> • A12 Use of health data for healthcare, research and policy marking • A13 Access of policy makers, regulators to health data • A14 Sharing / access to data
Participants	EU's Joint Action Towards the European Health Data Space (TEHDAS JA).
Moderator	Open Evidence

Workshop 3. Access and Governance of Health Data	
Date	19/04/2021
Area	Costs and benefits of primary use of health data, costs and benefits of access to health data for secondary purposes, and citizen access to health data
Objective	Fill the gaps identified in the gap analysis
Main RQs addressed	<ul style="list-style-type: none"> • A12 Use of health data for healthcare, research and policy marking • A13 Access of policy makers, regulators to health data • A14 Sharing / access to data
Participants	5 panel experts from <ul style="list-style-type: none"> • Data permit authorities • National governments bodies
Moderator	Open Evidence

Evaluation of Article 14 of Directive 2011/24/EU workshops

Workshop 1. Evaluation of the eHealth Network	
Date	04/03/2021
Area	eHealth Network evaluation
Objective	Fill the gaps identified in the gap analysis
Main RQs addressed	<ul style="list-style-type: none"> • A16 Application of Art. 14 and accompanying acts • A17 Effectiveness • A18 Efficiency • A19 Relevance • A20 Coherence • A21 EU added value
Participants	eHeath Network
Moderator	Open Evidence

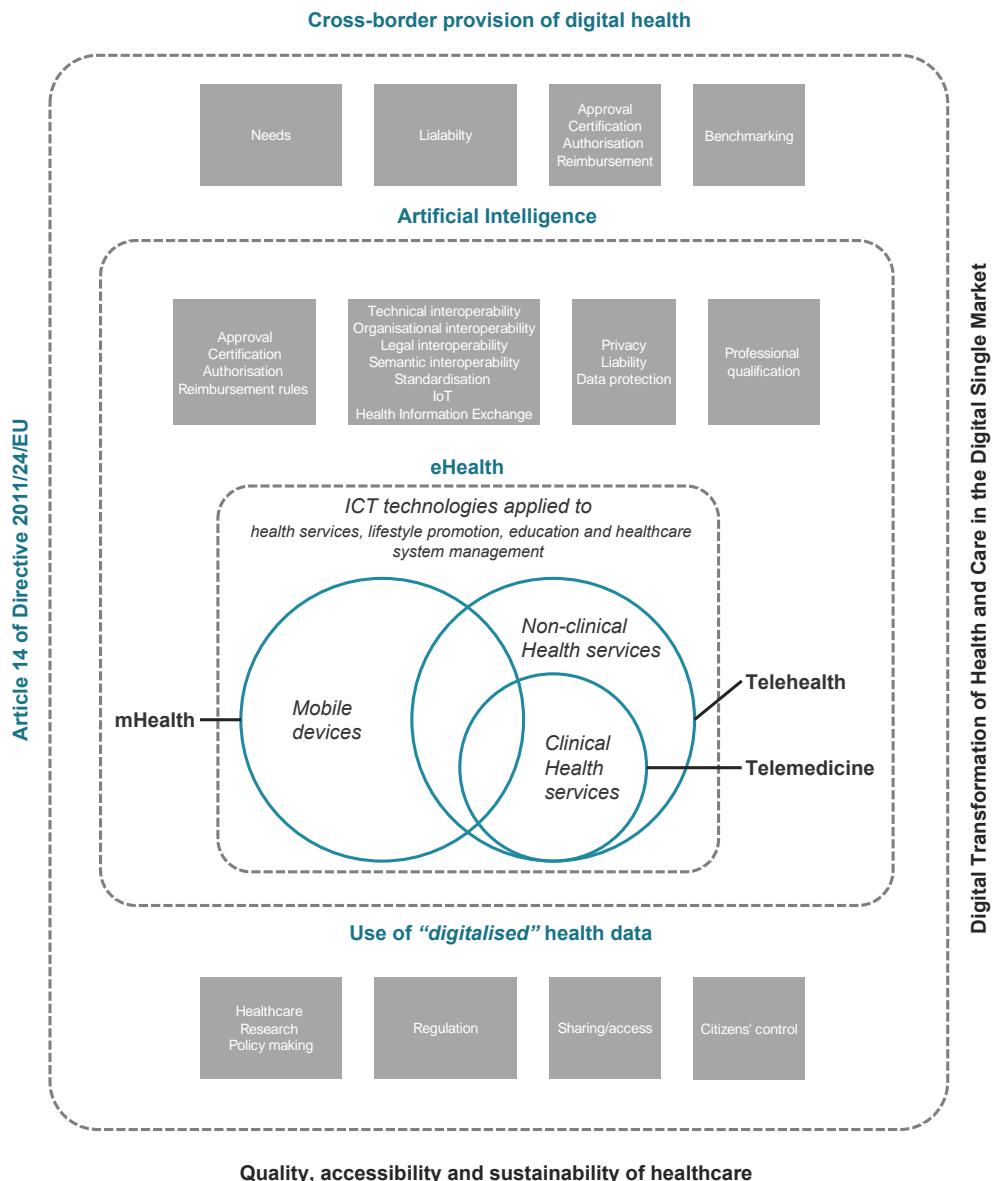
Workshop 2. The future of the eHealth Network	
Date	11/03/2021
Area	eHealth Network current and future needs
Objective	Define current and future needs in terms of cross-border healthcare provision
Main RQs addressed	<ul style="list-style-type: none"> • A16 Application of Art. 14 and accompanying acts • A17 Effectiveness • A18 Efficiency • A19 Relevance • A20 Coherence • A21 EU added value
Participants	Mixed pool of 7 experts on: <ul style="list-style-type: none"> • Interoperability of health data • mHealth/telemedicine • Cybersecurity • Former eHealth Network Members
Moderator	Open Evidence

8.3.3 Online questionnaires

[TO BE INCLUDED THE PDF]

8.4 Digital health products and services

8.4.1 eHealth scope



Source: Author elaboration

8.4.2 ePrescription

Doctors from these countries	Can access health data of citizens coming from
Croatia	Czech Republic (Sept. 2019), Malta (Feb. 2020) and Portugal (Feb. 2020)
Luxembourg	Czech Republic (Jun. 2019) and Malta (Dec. 2019)
Malta	Portugal (Feb. 2020)
Portugal	Malta (Jan. 2020)

Health data of citizens from	Can be consulted by doctors from (using Patient Summary)
Czech Republic	Luxembourg (Jun. 2019) and Croatia (Sept. 2019)
Malta	Luxembourg (Dec. 2019), Portugal (Jan. 2020) and Croatia (Feb. 2020)
Portugal	Malta (Feb. 2020), Croatia (Feb. 2020) and Luxembourg (March 2020)

8.4.3 Main medical standards (Schultz et al., 2019)

Standards development organisation	Standard	Scope
Federative Committee on Anatomical Terminology (FCAT)	Terminologia Anatomica (TA)	Anatomy terms in English and Latin
Health Level Seven (HL7)	v2	Messaging protocol; several of the chapters of this standard cover clinical content
	v3 (RIM)	Information ontology; especially the "Clinical Statement" work aims to create reusable clinical data standards
	CDA Level 1–3	Information model for clinical documents (embedding of terminology standards in level 2 and 3); especially the Continuity of Care Document (CCD) specifications and the Consolidated CDA (C-CDA) specifications add detail to standards for clinical documents
	FHIR	Information and Document model; several parts of the core specification deal with clinical content
Integrating the Healthcare Enterprise (IHE)	Several Integration profiles	Clinical workflows including references to clinical data standards to be used
International Organization for Standardization (ISO)	TS22220:2011	Identification of subjects of care
	21090:2011	Harmonized data types for information exchange
	13606	High-level description of clinical information models
	23940 (ContSys)	Health care processes for continuity of care
	14155	Clinical investigations
	IDMP	Medicinal products
National Electrical Manufacturers Association (NEMA)	DICOM	Medical imaging and related data
openEHR foundation	openEHR	Clinical information model specification
Regenstrief Institute	LOINC	Terminology for lab and other observables

Standards development organisation	Standard	Scope
	UCUM	Standardised representation of units of measure according to the SI units (ISO 80000)
PCHAlliance (Personal Connected Health Alliance)	Continua Design Guidelines	Collecting data from personal health devices
Standards development organisation	Standard	Scope
SNOMED International, formerly knowns as the International Health Terminology Standards Development Organisation	SNOMED CT	Terminology / Ontology for representing the electronic health record ("context model" = Information model for SNOMED CT)
World Health Organization (WHO)	ICD-10 / ICD-11	Disease classification
	ICF	Classification of functioning, disability and health
	ICHI	Health procedure classification
	INN	Generic names for pharmaceutical substances
	ATC	Drug ingredient classification
World Organization of Family Doctors (WONCA)	ICPC	Primary care classification

8.4.4 Focus areas of the Interoperability action plan

1. **Ensure governance, coordination and sharing of interoperability initiatives.** Realising interoperability of public administrations requires governance and coordination bodies, and processes for planning, implementing and using interoperability solutions, both nationally and across the Union.
The Commission and the Member States should implement the European interoperability framework. The Commission will monitor the implementation of the European interoperability framework through the ISA² programme
2. **Develop organisation interoperability solutions.** Businesses and citizens should be able to benefit from interoperable public services based on a better integration of business processes and exchange of information between public administrations in the Union.
3. **Engage stakeholders and raise awareness on interoperability.** Each interoperability initiative should be driven by a specific business case showing that interoperability is a worthwhile investment and that user needs are better fulfilled when information systems can communicate with each other.
4. **Develop, maintain and promote key interoperability enablers.** To improve the quality of European public services digitally delivered to end users, the Commission and Member States should define, develop, improve, make operational, maintain and promote a set of key interoperability enablers, while ensuring the security of exchanged data.
5. **Develop, maintain and promote instruments that support interoperability.** When designing, implementing and using interoperability solutions Member States need the support of practical instruments, i.e. tools, frameworks, guidelines and specifications, which are necessary for achieving interoperability at national level and across borders. The Commission and Member States should promote the reuse of existing instruments and further develop new ones, in particular:
 - . the European interoperability reference architecture and European interoperability cartography;
 - . ways of assessing the ICT implications of the Union law and identifying gaps in legislation hampering interoperability;
 - . the 'sharing and reuse framework for IT solutions' developed in the context of the ISA² programme, to promote and improve the sharing, collaborative development and reuse of IT solutions (including open

The Commission will support, promote and monitor the implementation of the interoperability action plan, and the European interoperability framework in general, primarily through the ISA² programme.^{source} by public administrations.

8.4.5 Draft Code of Conduct practical guidelines for app developers

In order to help mHealth applications developers to better understand and apply the new regulation on data protection, the European Commission facilitated the drafting of a draft code of conduct. Three instances will be part of the governance which remains to be defined, including one dedicated to tracking and monitoring accredited applications to ensure their continuous compliance.

The current draft includes guidelines on the following subjects: user consent, purpose limitation and data minimisation, privacy by design and by default, data subject rights and information requirements, data retention, security measures, advertising in mHealth apps, use of personal data for secondary purposes,

disclosing data to third parties for processing operations, data transfers, personal data breach, data gathered from children.

Developers who want to declare their adherence to the Code should complete the privacy impact assessment and a self-declaration of compliance to the Monitoring Body. Once checked and approved by the monitoring body, the application will be identified in a centralised public register. If willing, the developer can undergo under a third-party audit and certification of compliance. The monitoring body will randomly select accepted declaration to recheck the compliance.

This code of conduct should be the first step for labelling mHealth applications. However, it is still not in place.

The current draft includes guidelines on the following subjects:

- **User consent:** prior or as soon as users install an app, developers must obtain their free, specific and informed consent on his data's processing. The consent must be explicit, and the developer must be able to demonstrate that users have provided their consent.
- **Main principles** to respect before releasing an app: (1) purpose limitation, ie an app must be designed to only collect and process data concerning health for specific and legitimate purposes; (2) data minimisation, ie collection or processing are strictly limited to the quantity and duration necessary; (3) transparency and information of users; (4) privacy by design and by default, the privacy implications of the app have to be considered at each step of the development and wherever the user is given a choice and (5) data subject rights, users of the application have the right to access any personal data relating to them.
- **Preliminary information:** Developers must provide clear description of the purposes for which personal is processed and whether any data is stored in any other location than their device, they must also identify themselves clearly and provide contact information.
- **Data backup duration:** storage of personal data must be limited to the duration necessary for the functionalities of the apps
- **Security measures:** App developers should ensure the confidentiality, integrity and availability of the personal data processed via their apps
- **Advertising:** use of advertisements must be clearly authorised by the user before the app is installed
- **Disclosing data to third parties for processing operations:** The user needs to be informed prior to disclosure and the app developer needs to enter into a binding legal agreement with the third party.
- **Data transfers:** For data transfers to a location outside the EU/EEA, there needs to be legal guarantees permitting such transfer, e.g. an adequacy decision of the European Commission, European Commission Model Contracts or Binding Corporate Rules.
- **Personal data breach:** The Code provides a checklist to follow in case of a personal data breach, in particular the obligation to notify a data protection authority.
- **Data gathered from children:** Depending on the age limit defined in national legislation, the most restrictive data processing approach needs to be taken and a process to obtain parental consent needs to be put in place.

8.5 Governing the use of health data

8.5.1 Calculating value of health data

Estimated market value of health data per country. The calculations of this table were based off of the methodology and results of the EY 2019 report, "Realising the value of health care data: a framework for the future". In the EY report, the value of health data was calculated for the UK and the results were presented as low and high ranges of the value per patient record and the total market value.

In this report, the value of health data per patient health record was used as a baseline to estimate the value of a patient health record in other Member States. The methodology for this is as follows:

1. Population values were recorded for all MS.
2. The eHealth adoption indicator (EHR adoption indicator), from the "2018 Benchmarking Deployment of eHealth among General Practitioners" of the European Commission, was recorded for all Member States. This EHR composite indicator combines 23 functionalities across five sub dimensions (health info and data, clinical decision support system, order-entry and result management, image, administrative) to show the availability and adoption of EHRs across the EU. The EHR composite indicator shows that EHRs are fully available across the 27 EU countries; in some countries there is almost full adoption. For context, the EHR composite indicator score for the EU in 2018 was 3.196.
3. The percentage of health records/population was estimated for the UK using the number of primary health records (EY, 2019)/population. This gave a baseline of 83% of health records/population.
4. Using this 83% as a baseline, the number of primary health records for other Member States was calculated as follows

$$\frac{(\text{Population of Member State A}) * (\text{eHealth adoption of Member State A}) * (83\% \text{ primary health records for UK})}{(\text{eHealth adoption of UK})}$$

This results in the number of primary health records for Member State A.

5. The percentage of the number of primary health records for each Member State was calculated using the following:

$$\frac{\text{Number of primary health records of Member State A}}{\text{Population of Member State A}}$$

6. The low range of an EHR per patient was calculated using the value of an EHR per patient in the UK as a baseline (24EUR). The value of other EHRs per patient in other Member States is as follows:

$$\frac{(\text{€24 EHR value per patient in the UK}) * (\text{Percent of primary health records for Member State A})}{(83\% \text{ primary health records for UK})}$$

7. The low range of an EHR per patient in each Member State was multiplied by the Member State's respective PPP National currency units/Euro. This resulted in Market value in PPP National currency units/Euro per patient.
8. Steps 6-8 were repeated for the high range of an EHR per patient, using the UK as a baseline (217EUR)
9. The low range of the total market value of health data per Member State was calculated by the number of primary health records for each Member State by the low range of the value of EHR per patient.

10. Step 9 was repeated for the high range of the total market value of health data, using the high range value of EHR per patient.

For more calculations, please see the file "DG SANTE – Market Value of Health Data Calculations.xls" submitted along with this report.

Estimated total savings for Member States health services and benefits per patient per annum. The calculations of this table were based off of the methodology and results of the EY 2019 report, "Realising the value of health care data: a framework for the future". In the EY report, the value of health data was calculated for the UK and the results were presented as low and high ranges of the value per patient record and the total market value.

In this report, the value of health data per patient health record was used as a baseline to estimate the value of a patient health record in other Member States. The methodology for this is as follows:

1. Population values were recorded for all MS.
2. EHR adoption indicator, from the "2018 Benchmarking Deployment of eHealth among General Practitioners" of the European Commission, was recorded for all Member States. This EHR composite indicator combines 23 functionalities across five sub dimensions (health info and data, clinical decision support system, order-entry and result management, image, administrative) to show the availability and adoption of EHRs across the EU. The EHR composite indicator shows that EHRs are fully available across the 27 EU countries; in some countries there is almost full adoption. For context, the EHR composite indicator score for the EU in 2018 was 3.196.
3. The percentage of health records/population was estimated for the UK using the number of primary health records (EY, 2019)/population. This gave a baseline of 83% of health records/population.
4. Using this 83% as a baseline, the number of primary health records for other Member States was calculated as follows

$$\frac{(\text{Population of Member State A}) * (\text{eHealth adoption of Member State A}) * (83\% \text{ primary health records for UK})}{(\text{eHealth adoption of UK})}$$

This results in the number of primary health records for Member State A.

1. The percentage of the number of primary health records for each Member State was calculated using the following:

$$\frac{\text{Number of primary health records of Member State A}}{\text{Population of Member State A}}$$

2. The total savings for Member State health services per annum was calculated using the value of the savings for UK health services (NHS) as a baseline (5,650,000,000). The value of other EHRs per patient in other Member States is as follows:

$$\frac{(\text{€}5,650,000,000 \text{ total NHS savings in the UK}) * (\text{Percent of primary health records for Member State A})}{(83\% \text{ primary health records for UK})}$$

3. The total savings for Member State health services per annum was multiplied by the Member State's respective PPP National currency units/Euro. This resulted in Total savings for Member State health services per annum in PPP National currency units/Euro per patient (millions).
4. Steps 6-8 were repeated for the total benefits for patients per annum, using the UK as a baseline (5,198,000,000)

Estimated fixed costs of data permit authorities. The fixed costs for setting up a data permit authority were extrapolated in this report using Findata as a baseline. In 2019, the Finnish Government allocated 2.5 million euros for the year to launch the operations of the data permit authority and the construction of a data-secure environment. The budget is about 1 million euros per year, though it is higher in the beginning years 2019-2021 (EC, 2020).

1. Steps 1-5 of table “Estimated market value of health data per country” were repeated.
2. Using 87% as a baseline, which are the estimated primary health records over population for Finland, the estimated fixed cost of other data permit authorities in other Member States is as follows:

$$\frac{(\text{€}2,500,000 \text{ fixed cost for Findata}) * (\text{Percent of primary health records for Member State A})}{(87\% \text{ primary health records for UK})}$$

The estimated fixed cost of data permit authorities in each Member State was multiplied by the Member State’s respective PPP National currency units/Euro. This resulted in a value of PPP National currency units/Euro.

Estimated variable costs of data permit authorities. The variable costs of a data permit authority were extrapolated in this report using Findata as a baseline. The variable costs used are detailed in Box 40 Examples of fees for Findata data permits and requests.

1. All Finnish variable costs were converted to PPP national currency units /Euro.
2. The estimated variable cost of data permit authorities in each Member State was multiplied by the Member State’s respective PPP National currency units/Euro. This resulted in a value of PPP National currency units/Euro.

This step was repeated for each low and high range of the Finnish variable costs.

8.5.2 Estimated economic value of health data

Electronic Health Record (EHR) adoption

The values shown in Table 64 represent the estimated economic value for Member States based off their functionality and level of EHRs. These values were estimated by taking into consideration population, the number of health records, and the EHR adoption index, which was calculated in the 2018 Benchmarking Deployment of eHealth among General Practitioners. The estimated economic value per patient, when considering the average EHR adoption index for the EU, ranges from 5 to 49 PPP national currency units/Euro. The estimated savings in PPP national currency units/Euro range between 1.8 billion to 16.6 billion when considering the average EHR adoption index across the EU. Each of the four sub-index (EHR, HIE, Telehealth and Personal Health Record) contributes 25% to the total composite index (eHealth adoption index). Therefore, the final value was multiplied by 0.25. This economic value derives from benefits of the 5 EHR adoption composite indicator subdimensions: (1) health info and data, (2) clinical decision support system, (3) order-entry and result management, (4) image, and (5) administrative. There are 23 functionalities among these subdimensions and include symptoms, reasons for appointment, clinical notes, vital signs, treatment, history, medication list, drug-allergy alerts, radiology test images, and finances/billing.

Table 64. Estimated economic value of heath data - EHR adoption

country	population (2018)**	EHR adoption (2018)** *	# of primary health records	€ value low range per patient	€ value high range per patien t	% EHR / populatio n	PPP National currency units*** *	PPP National currenc y units/ Euro	Value in PPP National currency units / Euro per patient	Value in PPP National currency units / Euro per patient	Total value in PPP National currency units / Euro (millions)	
									low range	high range	low range	high range
Austria	8,840,521	2.975	6,341,875	21	188	72%	112.6	1.09	6	51	33	298
Belgium	11,427,054	3.203	8,825,596	22	203	77%	114.5	1.11	6	56	49	447
Bulgaria	6,951,482	2.745	4,601,216	19	174	66%	51.7	0.5	2	22	22	200
Croatia	4,087,843	3.085	3,040,900	21	195	74%	70.5	0.69	4	33	16	148
Cyprus	1,189,265	2.728	782,305	19	172	66%	90.4	0.88	4	38	4	34
Czechia	10,629,928	3.114	7,981,817	22	197	75%	73.9	0.72	4	35	43	393
Denmark	5,793,636	3.47	4,847,675	24	219	84%	141.9	1.38	8	76	29	266
Estonia	1,321,977	3.522	1,122,706	24	223	85%	83.4	0.81	5	45	7	62
Finland	5,515,525	3.281	4,363,610	23	207	79%	125.5	1.22	7	63	25	226
France	67,320,216	3.331	54,072,065	23	211	80%	113.8	1.11	6	58	311	2,847
Germany	82,905,782	3.082	61,612,706	21	195	74%	106.1	1.03	5	50	328	3,001
Greece	10,732,882	2.297	5,944,703	16	145	55%	86.6	0.84	3	31	24	216

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

country	population (2018)**	EHR adoption (2018)** *	# of primary health records	€ value low range per patient	€ value high range per patient	% EHR / populatio n	PPP National currency units*** *	PPP National currenc y units/ Euro	Value in PPP National currency units / Euro per patient		Total value in PPP National currency units / Euro (millions)	
									low range	high range	low range	high range
Hungary	9,775,564	2.951	6,956,069	20	187	71%	65.9	0.64	3	30	35	324
Ireland	4,867,316	3.406	3,997,487	24	215	82%	134.1	1.3	8	70	24	215
Italy	60,421,760	3.356	48,895,416	23	212	81%	103.2	1	6	53	284	2,594
Latvia	1,927,174	2.343	1,088,795	16	148	56%	76.6	0.74	3	28	4	40
Lithuania	2,801,543	2.183	1,474,701	15	138	53%	67.4	0.66	2	23	6	51
Luxembourg	607,950	2.866	420,143	20	181	69%	130	1.26	6	57	2	19
Malta	484,630	2.4	280,462	17	152	58%	86.2	0.84	3	32	1	11
Netherlands *	17,231,624	3.5	14,542,768	24	221	84%	114.2	1.11	7	61	88	804
Poland	37,974,750	2.635	24,128,391	18	167	64%	59.5	0.58	3	24	110	1,005
Portugal	10,283,822	3.062	7,592,985	21	194	74%	88.1	0.86	5	41	40	367
Romania	19,472,545	2.608	12,245,686	18	165	63%	55.7	0.54	2	22	55	505
Slovakia	5,446,771	2.74	3,598,674	19	173	66%	84.2	0.82	4	35	17	156
Slovenia	2,073,894	2.504	1,252,200	17	158	60%	87.1	0.85	4	34	5	50
Spain	46,797,754	3.384	38,186,354	23	214	82%	96.5	0.94	5	50	223	2,042
Sweden	10,175,214	3.216	7,890,643	22	203	78%	125.1	1.22	7	62	44	401
EU-27	447,058,422	2.962	336,087,947	22	197	75%	102.9	1.00	5	49	1,811	16,561
United Kingdom (baseline)	66,460,344	3.432	55,000,000	24	217	83%	119.3	1.16	7	63	326	2,983

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement.

** Source: The World Bank website <https://data.worldbank.org/>

*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.

**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the beforementioned source and divided by the EU 2018 average of 102.9.

Health Information Exchange (HIE) adoption

Health information exchange is the process of electronically transferring / sharing / enabling access to patient health information and data (EC, 2018) and in this case if used as a proxy for interoperability for primary care purposes. The values shown in Table 65 represent the estimated economic value for Member States based off their level of HIE. The estimated value for patients ranges from 2 PPP national currency units/Euro (low range for Bulgaria and Romania) to 11 as the high range for Denmark. The differences in the value of EHRs per patient differs by Member State due to their HIE adoption index, population, and differences in living costs. The estimated savings in PPP national currency units/Euro range between 1.3 billion to 12.4 billion when considering the average HIE adoption index across the EU. These savings could come from a decreased disease and economic burden through HIE practices. These values were estimated by taking into consideration population, the number of health records, and the health information exchange (HIE) adoption index, which was calculated in the 2018 Benchmarking Deployment of eHealth among General Practitioners. The HIE adoption composite indicator is divided into 3 subdimensions: (1) clinical data, (2) patient administration, (3) management. There are 13 functionalities among these subdimensions and include exchanging patient medication lists with other healthcare professionals/providers, exchanging medical patient data with other healthcare professionals/ providers, and sending/receiving referral and discharge letters, among others for clinical data. For patient administration, the functionalities are the following: certifying sick leaves, certifying disabilities, performing patient appointment requests. For management, the functionalities are exchanging administrative patient data with reimburses or other care providers and ordering supplies for the GP's own practice.

Table 65. Estimated economic value of heath data - Health Information Exchange (HIE) adoption

country	population (2018)**	HIE adoption (2018)***	# of primary health records	€ value low range per patient	€ value high range per patient	% PHR adoption by patients/ population	PPP National currency units****	PPP National currency units/ Euro	Estimated value in PPP National currency units/Euro per patient		Estimated savings in PPP National currency units/Euro (millions)	
									low range	high range	low range	high range
Austria	8,840,521	1.203	3,624,891	12	108	41%	112.6	1.09	5	42	22	198
Belgium	11,427,054	1.302	5,071,036	13	116	44%	114.5	1.11	6	55	46	422
Bulgaria	6,951,482	1.238	2,933,253	12	111	42%	51.7	0.5	2	17	13	122
Croatia	4,087,843	1.514	2,109,461	15	135	52%	70.5	0.69	4	34	17	152
Cyprus	1,189,265	1.191	482,772	12	106	41%	90.4	0.88	3	32	3	24
Czechia	10,629,928	1.421	5,148,442	14	127	48%	73.9	0.72	3	29	30	271
Denmark	5,793,636	2.673	5,278,391	26	239	91%	141.9	1.38	11	100	51	463
Estonia	1,321,977	2.417	1,089,060	24	216	82%	83.4	0.81	6	57	11	98
Finland	5,515,525	2.576	4,842,662	25	230	88%	125.5	1.22	8	69	29	267

country	population (2018)**	HIE adoption (2018)***	# of primary health records	€ value low range per patient	€ value high range per patient	% PHR adoption by patients/ population	PPP National currency units****	PPP National currency units/ Euro	Estimated value in PPP National currency units/Euro per patient		Estimated savings in PPP National currency units/Euro (millions)	
									low range	high range	low range	high range
France	67,320,216	1.281	29,393,145	13	114	44%	113.8	1.11	5	49	221	2,024
Germany	82,905,782	1.4	39,560,728	14	125	48%	106.1	1.03	4	38	188	1,714
Greece	10,732,882	1.389	5,081,244	14	124	47%	86.6	0.84	3	27	18	163
Hungary	9,775,564	1.327	4,421,444	13	119	45%	65.9	0.64	3	25	26	236
Ireland	4,867,316	1.137	1,886,259	11	102	39%	134.1	1.3	6	58	16	149
Italy	60,421,760	1.549	31,900,406	15	138	53%	103.2	1	5	45	203	1,857
Latvia	1,927,174	1.419	932,083	14	127	48%	76.6	0.74	3	28	5	42
Lithuania	2,801,543	1.344	1,283,358	13	120	46%	67.4	0.66	3	25	7	62
Luxembourg	607,950	1.386	287,199	14	124	47%	130	1.26	4	40	1	9
Malta	484,630	1.414	233,567	14	126	48%	86.2	0.84	3	27	1	7
Netherlands*	17,231,624	2.067	12,139,984	20	185	70%	114.2	1.11	6	58	79	725
Poland	37,974,750	1.455	18,832,559	14	130	50%	59.5	0.58	2	17	57	524
Portugal	10,283,822	1.754	6,148,024	17	157	60%	88.1	0.86	4	41	39	355
Romania	19,472,545	1.186	7,871,524	12	106	40%	55.7	0.54	2	18	37	342
Slovakia	5,446,771	1.133	2,103,393	11	101	39%	84.2	0.82	3	25	8	75
Slovenia	2,073,894	1.719	1,215,105	17	154	59%	87.1	0.85	4	34	6	52
Spain	46,797,754	1.763	28,120,869	17	158	60%	96.5	0.94	5	49	213	1,952
Sweden	10,175,214	2.354	8,163,971	23	210	80%	125.1	1.22	8	73	61	561
EU-27	447,058,422	2.017	290,661,778	19	170	65%	102.9	1.00	5	43	1,355	12,387
United Kingdom (baseline)	66,460,344	2.428	55,000,000	24	217	83%	119.3	1.16	7	63	326	2,983

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement between Slovenia and Estonia.

** Source: The World Bank website <https://data.worldbank.org/>

*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.

**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the aforementioned source and divided by the EU 2018 average of 102.9.

Telehealth adoption

The values shown in Table 66 represent the economic value for Member States based off their level of telehealth adoption. It is important to note that, in most cases, the cost for patients is the same as an office visit. However, healthcare efficiencies and cost are impacted positively due to fewer transports to hospital ER's, hospital admissions, shorter hospital stays, reduced travel times, and improved management of chronic diseases which translates into an estimated EU economic value for telehealth adoption valued at 1.2 billion and 11.3 billion PPP currency units/ Euro. The telehealth adoption composite indicator, which is a factor in the differences of value between Member States, is divided into 2 subdimensions: (1) clinical practice and (2) training. There are two functions in each subdimension: monitoring patients remotely at their homes and consultations with patients for the clinical practice subdimension, and training/education and consultations with other healthcare practitioners for the training subdimension. These values were estimated by taking into consideration population, the percentage of telemedicine used in MS, and the telehealth adoption index, which was calculated in the 2018 Benchmarking Deployment of eHealth among General Practitioners. The UK was used as a baseline with about 47% of clinicians using telemedicine (Deloitte, 2020).

Table 66. Estimated economic value of health data - Telehealth adoption

country	population (2018)**	telehealth adoption (2018)***	€ value low range per patient	€ value high range per patient	% telehealth / population	PPP National currency units****	PPP National currency units/ Euro	Value in PPP National currency units/Euro per patient	Total value in PPP National currency units/Euro (millions)		
Austria	8,840,521	1.679	24	215	47%	112.6	1.09	6	59	24	222
Belgium	11,427,054	1.412	20	181	39%	114.5	1.11	6	50	22	203
Bulgaria	6,951,482	1.654	23	212	46%	51.7	0.5	3	27	19	169
Croatia	4,087,843	1.824	26	234	51%	70.5	0.69	4	40	13	121
Cyprus	1,189,265	1.998	28	256	56%	90.4	0.88	6	56	5	42
Czechia	10,629,928	1.773	25	227	49%	73.9	0.72	4	41	33	298
Denmark	5,793,636	1.951	27	250	54%	141.9	1.38	9	86	21	196
Estonia	1,321,977	1.93	27	247	54%	83.4	0.81	5	50	5	44
Finland	5,515,525	2.107	30	270	59%	125.5	1.22	9	82	24	218
France	67,320,216	1.5	21	192	42%	113.8	1.11	6	53	148	1,349
Germany	82,905,782	1.535	22	197	43%	106.1	1.03	6	51	190	1,740
Greece	10,732,882	1.808	25	232	50%	86.6	0.84	5	49	34	312
Hungary	9,775,564	1.996	28	256	55%	65.9	0.64	4	41	38	347
Ireland	4,867,316	1.789	25	229	50%	134.1	1.3	8	75	15	139

country	population (2018)**	telehealth adoption (2018)***	€ value low range per patient	€ value high range per patient	% telehealth / population	PPP National currency units****	PPP National currency units/ Euro	Value in PPP National currency units/Euro per patient		Total value in PPP National currency units/Euro (millions)	
								low range	high range	low range	high range
Italy	60,421,760	1.709	24	219	47%	103.2	1	6	55	172	1,572
Latvia	1,927,174	1.572	22	202	44%	76.6	0.74	4	38	5	42
Lithuania	2,801,543	1.256	18	161	35%	67.4	0.66	3	26	4	39
Luxembourg	607,950	1.378	19	177	38%	130	1.26	6	56	1	10
Malta	484,630	1.515	21	194	42%	86.2	0.84	4	41	1	10
Netherlands*	17,231,624	2.124	30	272	59%	114.2	1.11	8	76	76	692
Poland	37,974,750	1.726	24	221	48%	59.5	0.58	3	32	110	1,007
Portugal	10,283,822	1.425	20	183	40%	88.1	0.86	4	39	20	186
Romania	19,472,545	1.759	25	226	49%	55.7	0.54	3	31	59	537
Slovakia	5,446,771	1.705	24	219	47%	84.2	0.82	5	45	15	141
Slovenia	2,073,894	1.788	25	229	50%	87.1	0.85	5	49	6	59
Spain	46,797,754	1.888	26	242	52%	96.5	0.94	6	57	162	1,486
Sweden	10,175,214	1.731	24	222	48%	125.1	1.22	7	67	30	272
EU-27	447,058,422	1.723	24	216	47%	102.9	1.00	6	54	1,238	11,322
United Kingdom (baseline)	66,460,344	1.692	24	217	47%	119.3	1.16	7	63	326	2,983

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement between Estonia and Finland.

** Source: The World Bank website <https://data.worldbank.org/>

*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.

**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the beforementioned source and divided by the EU 2018 average of 102.9.

Personal Health Records

The value of functionality and availability of patients to use and access their personal health records is shown in Table 67. The value of the personal health records (PHR) table represents the economic value of ICT systems that general practitioners can use to allow their patients to access the following six different types of PHR functionality: (1) request appointments, (2) view their medical records, (3) view test results, (4) request referrals, (5) supplement their medication, (6) request renewals or prescriptions. These values were estimated by taking into consideration population, the number of health records, and the PHR adoption index, which was calculated in the 2018 Benchmarking Deployment of eHealth among General Practitioners. The estimated EU saving for the adoption of PHR access and use, ranges between 849 million to 7.8 billion PPP national currency units /Euro, which considers the average PHR adoption index across Member States.

Table 67. Estimated economic value of heath data - Personal Health Record (PHR) adoption

country	population (2018)**	PHR adoption (2018)***	# of primary health records	€ value low range per patient	€ value high range per patient	% PHR adoption by patients/ population	PPP National currency units****	PPP National currency units/ Euro	Estimated value in PPP National currency units/Euro per patient		Estimated savings in PPP National currency units/Euro (millions)	
									low range	high range	low range	high range
Austria	8,840,521	1.203	3,624,891	12	108	41%	112.6	1.09	3	29	11	97
Belgium	11,427,054	1.302	5,071,036	13	116	44%	114.5	1.11	4	32	16	148
Bulgaria	6,951,482	1.238	2,933,253	12	111	42%	51.7	0.5	2	14	9	81
Croatia	4,087,843	1.514	2,109,461	15	135	52%	70.5	0.69	3	23	8	71
Cyprus	1,189,265	1.191	482,772	12	106	41%	90.4	0.88	3	23	1	13
Czechia	10,629,928	1.421	5,148,442	14	127	48%	73.9	0.72	2	23	18	163
Denmark	5,793,636	2.673	5,278,391	26	239	91%	141.9	1.38	9	82	34	315
Estonia	1,321,977	2.417	1,089,060	24	216	82%	83.4	0.81	5	44	6	59
Finland	5,515,525	2.576	4,842,662	25	230	88%	125.5	1.22	8	70	30	279
France	67,320,216	1.281	29,393,145	13	114	44%	113.8	1.11	3	32	92	841
Germany	82,905,782	1.4	39,560,728	14	125	48%	106.1	1.03	4	32	135	1,237
Greece	10,732,882	1.389	5,081,244	14	124	47%	86.6	0.84	3	26	17	158
Hungary	9,775,564	1.327	4,421,444	13	119	45%	65.9	0.64	2	19	14	131
Ireland	4,867,316	1.137	1,886,259	11	102	39%	134.1	1.3	4	33	5	48
Italy	60,421,760	1.549	31,900,406	15	138	53%	103.2	1	4	35	121	1,104
Latvia	1,927,174	1.419	932,083	14	127	48%	76.6	0.74	3	24	3	30
Lithuania	2,801,543	1.344	1,283,358	13	120	46%	67.4	0.66	2	20	4	39
Luxembourg	607,950	1.386	287,199	14	124	47%	130	1.26	4	39	1	9

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

Malta	484,630	1.414	233,567	14	126	48%	86.2	0.84	3	26	1	7
Netherlands*	17,231,624	2.067	12,139,984	20	185	70%	114.2	1.11	6	51	61	561
Poland	37,974,750	1.455	18,832,559	14	130	50%	59.5	0.58	2	19	67	612
Portugal	10,283,822	1.754	6,148,024	17	157	60%	88.1	0.86	4	34	26	241
Romania	19,472,545	1.186	7,871,524	12	106	40%	55.7	0.54	2	14	23	209
Slovakia	5,446,771	1.133	2,103,393	11	101	39%	84.2	0.82	2	21	6	53
Slovenia	2,073,894	1.719	1,215,105	17	154	59%	87.1	0.85	4	33	5	47
Spain	46,797,754	1.763	28,120,869	17	158	60%	96.5	0.94	4	37	121	1,108
Sweden	10,175,214	2.354	8,163,971	23	210	80%	125.1	1.22	7	64	47	429
EU-27	447,058,422	1.578	230,154,831	15	135	51%	102.9	1.00	4	34	849	7,767
United Kingdom (baseline)	66,460,344	2.428	55,000,000	24	217	83%	119.3	1.16	7	63	326	2,983

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement between Slovenia and Estonia.

** Source: The World Bank website <https://data.worldbank.org/>

*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.

**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the beforementioned source and divided by the EU 2018 average of 102.9.

8.5.3 Cost of cybersecurity breaches

Estimated cost of cybersecurity breaches. The calculations of this table in the Annex were based off of the methodology of the EY 2019 report, "Realising the value of health care data: a framework for the future" and the black market value of patient data in Czeschik's report "Black Market Value of Patient Data".

In this report, the black market value of health data per patient health record in the United States was used as a baseline to estimate the black market value of a patient health record in Member States. The methodology for this is as follows:

1. Steps 1-5 of table "Estimated market value of health data per country" were repeated.
2. The low range of an EHR per patient was calculated using the black market value of an EHR per patient in the US as a baseline (0.40EUR).
3. The black market value of other EHRs per patient in other Member States is as follows:
*(€0.04 EHR value per patient in the US) * (PPP National currency units / Euro of Member State A)*
4. The low range of the black market value of an EHR per patient in each Member State was multiplied by the Member State's respective PPP National currency units/Euro. This resulted in Market value in PPP National currency units/Euro per patient.
5. Steps 3-4 were repeated for the high range of an EHR per patient, using the US as a baseline (42EUR)
6. The low range of the total black market value of health data per Member State was calculated by the number of primary health records for each Member State by the low range of the black market value of EHR per patient (in PPP national currency units/euro).
7. Step 6 was repeated for the high range of the total black market value of health data, using the high range of the black market value of EHR per patient.

Table 68. Estimated cost of cybersecurity breaches

Country	Population (2018)	eHealth adoption (2018)	# of primary health records	% health records/ population	PPP National currency units/ Euro	Black market value in PPP National currency units/Euro per patient		Black market value in PPP National currency units/Euro (thousands)	
						Low range	High range	Low range	High range
Austria	8,840,521	1.914	5,563,354	63%	1.09	0.05	46	0.26	258
Belgium	11,427,054	2.067	7,765,897	68%	1.11	0.05	47	0.37	366
Bulgaria	6,951,482	1.809	4,134,594	59%	0.50	0.02	21	0.09	88
Croatia	4,087,843	2.180	2,930,000	72%	0.69	0.03	29	0.09	85
Cyprus	1,189,265	1.934	756,227	64%	0.88	0.04	37	0.03	28
Czechia	10,629,928	2.063	7,210,186	68%	0.72	0.03	30	0.22	219
Denmark	5,793,636	2.862	5,451,772	94%	1.38	0.06	58	0.32	319
Estonia	1,321,977	2.785	1,210,503	92%	0.81	0.03	34	0.04	42
Finland	5,515,525	2.644	4,794,741	87%	1.22	0.05	52	0.25	248
France	67,320,216	2.054	45,463,496	68%	1.11	0.05	47	2.13	2,131
Germany	82,905,782	1.941	52,908,719	64%	1.03	0.04	44	2.31	2,312
Greece	10,732,882	1.785	6,298,998	59%	0.84	0.04	36	0.22	225
Hungary	9,775,564	2.028	6,518,185	67%	0.64	0.03	27	0.18	177
Ireland	4,867,316	2.103	3,365,470	69%	1.30	0.06	55	0.19	186
Italy	60,421,760	2.185	43,407,193	72%	1.00	0.04	42	1.84	1,845
Latvia	1,927,174	1.826	1,157,014	60%	0.74	0.03	32	0.04	36
Lithuania	2,801,543	1.647	1,517,078	54%	0.66	0.03	28	0.04	42
Luxembourg	607,950	1.776	354,999	58%	1.26	0.05	54	0.02	19
Malta	484,630	1.695	270,083	56%	0.84	0.04	35	0.01	10
Netherlands	17,231,624	2.121	12,016,660	70%	1.11	0.05	47	0.57	565
Poland	37,974,750	1.837	22,936,174	60%	0.58	0.02	25	0.56	562
Portugal	10,283,822	2.118	7,161,391	70%	0.86	0.04	36	0.26	260
Romania	19,472,545	1.788	11,447,407	59%	0.54	0.02	23	0.26	263
Slovakia	5,446,771	1.756	3,144,709	58%	0.82	0.03	35	0.11	109
Slovenia	2,073,894	1.998	1,362,382	66%	0.85	0.04	36	0.05	49
Spain	46,797,754	2.365	36,389,245	78%	0.94	0.04	40	1.45	1,446

Study on Health Data, Digital Health and Artificial Intelligence in Healthcare

Country	Population (2018)	eHealth adoption (2018)	# of primary health records	% health records/ population	PPP National currency units/ Euro	Black market value in PPP National currency units/Euro per patient		Black market value in PPP National currency units/Euro (thousands)	
						Low range	High range	Low range	High range
Sweden	10,175,214	2.522	8,437,339	83%	1.22	0.05	52	0.43	435
United States (baseline)					1.12	.04	42		

* Netherlands was omitted in 2018 benchmark. The most recent benchmark was from 2013 and therefore the value has been estimated, with the assumption that this country remained in its 2013 placement between Estonia and Finland.
** Source: The World Bank website <https://data.worldbank.org/>
*** Source: European Commission. (2018). Benchmarking Deployment of eHealth among General Practitioners. <https://doi.org/10.2759/511610>.
**** Source: eurostat Data Browser. (2018). Eurostat. <https://ec.europa.eu/eurostat/databrowser/view/tec00120/default/table?lang=en>. The values are taken from the beforementioned source and divided by the EU 2018 average of 102.9.

Source: Authors' elaboration

8.6 Evaluation of Article 14 of Directive 2011/24/EU

8.6.1 Evaluation matrix

Criteria	Research questions (RQ)	Indicators	Source
Application of Art. 14 and accompanying acts (A16)	<ul style="list-style-type: none"> How effective was the setting up of the eHealth Digital Service Infrastructure in stimulating interoperability and cross-border exchange of health data? 	<ul style="list-style-type: none"> Number of Countries with Operational NCPeH Number of transactions between Countries 	<ul style="list-style-type: none"> eHDSI Monitoring Framework (KPIs)
	<ul style="list-style-type: none"> To what extent was the intervention of the eHealth Network effective in stimulating the use of health data for research and policy making? 	<ul style="list-style-type: none"> Number of publications using health data generated as a result of eHealth Network activities Number of policies and initiatives using health data generated as a result of eHealth Network activities 	<ul style="list-style-type: none"> Desk research
	<ul style="list-style-type: none"> To what extent was the intervention of the eHealth Network effective in stimulating the primary and secondary use of health data? 	<p>Primary use of data:</p> <ul style="list-style-type: none"> Number of ePrescriptions exchanged Number of Patient Summaries exchanged Number of Operational eP-A services Number of Operational eP-B services Number of Operational PS-A services Number of Operational PS-B services <p>Secondary use of data: NA</p>	<ul style="list-style-type: none"> eHDSI Monitoring Framework (KPIs)
	<ul style="list-style-type: none"> To what extent was the eHealth Network effective in supporting the use of health data for medical diagnosis and treatment, public health (including planning, provision of healthcare, management of health or social care systems and services, regulatory purposes, approval of medical devices, protecting against cross-border health threats) and for scientific or historical research and innovation? 	<ul style="list-style-type: none"> Number of publications using health data generated as a result of eHealth Network activities 	<ul style="list-style-type: none"> Desk research
	<ul style="list-style-type: none"> What were the factors that influenced the observed achievements and to what extent? 	<ul style="list-style-type: none"> Factors affecting the up-take rate of the developed tools and guidelines 	<ul style="list-style-type: none"> Focus Group Interviews
	<ul style="list-style-type: none"> Which factors hindered the attainment of the objectives and to what extent? How do these factors link to the actions carried out under Article 14? To what extent were there external factors that influenced the results? 	<ul style="list-style-type: none"> Factors affecting the up-take rate of the developed tools and guidelines 	<ul style="list-style-type: none"> Focus Group Interviews
Effectiveness (A17)	<ul style="list-style-type: none"> To what extent were the objectives reached, as they were set out in Article 14 (2) of the Directive? 	<ul style="list-style-type: none"> Number of information exchanged Number of guidelines produced on patient's summary and medical information for public health and research 	eHealth Network deliverables

Criteria	Research questions (RQ)	Indicators	Source
	<ul style="list-style-type: none"> What were the qualitative and quantitative effects of the eHealth Network on the cooperation and exchange of information between MS? How were these effects achieved? 	<ul style="list-style-type: none"> Adoption of guidelines on ePrescription, patient's summary and eID Number of Countries with Operational NCPeH Number of transactions between Countries Number of services offered on the MyHealth@EU platform 	eHDSI Monitoring Framework (KPIs)
	<ul style="list-style-type: none"> To what extent can they be attributed to the eHealth Network, e-Prescriptions and Patient Summaries, European Electronic Health Record exchange format, etc.? 	<ul style="list-style-type: none"> Number of ePrescriptions exchanged Number of Patient Summaries exchanged 	eHDSI Monitoring Framework (KPIs)
	<ul style="list-style-type: none"> How effective was the setting up of the eHealth Digital Service Infrastructure in stimulating interoperability and cross-border exchange of health data? 	<ul style="list-style-type: none"> Number of Operational eP-A services Number of Operational eP-B services Number of Operational PS-A services Number of Operational PS-B services 	eHDSI Monitoring Framework (KPIs)
	<ul style="list-style-type: none"> To what extent was the intervention of the eHealth Network effective in stimulating the use of health data for research and policy marking? 	<ul style="list-style-type: none"> Number of publications using health data generated as a result of eHealth Network activities Number of policies and initiatives using health data generated as a result of eHealth Network activities 	<ul style="list-style-type: none"> Desk research
	<ul style="list-style-type: none"> To what extent was the intervention of the eHealth Network effective in stimulating the primary and secondary use of health data? 	<p>Primary use of data:</p> <ul style="list-style-type: none"> Number of Countries with Operational NCPeH Number of transactions between Countries <p>Secondary use of data: NA</p>	eHDSI Monitoring Framework (KPIs)
	<ul style="list-style-type: none"> To what extent was the eHealth Network effective in supporting the use of health data for medical diagnosis and treatment, public health (including planning, provision of healthcare, management of health or social care systems and services, regulatory purposes, approval of medical devices, protecting against cross-border health threats) and for scientific or historical research and innovation? 	<ul style="list-style-type: none"> Number of publications using health data generated as a result of eHealth Network activities 	<ul style="list-style-type: none"> Desk research
	<ul style="list-style-type: none"> What were the factors that influenced the observed achievements and to what extent? Which factors hindered the attainment of the objectives and to what extent? How do these factors link to the actions carried out under Article 14? To what extent were there external factors that influenced the results? 	<ul style="list-style-type: none"> Factors affecting the up-take rate of the developed tools and guidelines Factors affecting the up-take rate of the developed tools and guidelines 	<ul style="list-style-type: none"> Focus Group Interviews

Criteria	Research questions (RQ)	Indicators	Source
Efficiency (A18)	<ul style="list-style-type: none"> To what extent have the actions carried out under Article 14 been realised in a cost-effective way? 	<ul style="list-style-type: none"> Costs of Joint Actions CEF funds Costs of DG RTD projects directly related to eHealth Network activities MD of eHealth Network members MS cost of implementation of developed tools DG REFORM capacity building budget Estimated benefits for the EU, Member States, Patients, HCP, Researchers, Industry. 	<ul style="list-style-type: none"> eHealth Network Joint Action budget CEF budget Relevant DG RTD projects' budget Accounting of MD spent (currently not monitored) Accounting of funds invested by MS in implementing the tools developed (currently not monitored) Estimation of benefits: https://ehealth-impact.eu/
	<ul style="list-style-type: none"> Looking closely at both the costs and benefits of Article 14 as they accrue to different eHealth stakeholders, how efficient has the implementation of Article 14 been for each type of stakeholder (citizens, patients, healthcare professionals, policy makers, researchers, companies (pharmaceutical sector, AI etc.)?)? 	<ul style="list-style-type: none"> Analysis of costs and benefits 	<ul style="list-style-type: none"> Survey
	<ul style="list-style-type: none"> To what extent are the costs justified and proportionate given the effects observed/objectives achieved/ benefits obtained in general? How proportionately were the costs of the intervention borne by different stakeholder groups taking into account the distribution of the associated benefits? 	<ul style="list-style-type: none"> Costs of Joint Actions CEF funds Costs of DG RTD projects directly related to eHealth Network activities MD of eHealth Network members MS cost of implementation of developed tools DG REFORM capacity building budget Estimated benefits for the EU, Member States, Patients, HCP, Researchers, Industry. 	<ul style="list-style-type: none"> eHealth Network Joint Action budget CEF budget Relevant DG RTD projects' budget Accounting of MD spent (currently not monitored) Accounting of funds invested by MS in implementing the tools developed (currently not monitored) DG REFORM funds invested on capacity building Estimation of benefits: https://ehealth-impact.eu/

Criteria	Research questions (RQ)	Indicators	Source
	<ul style="list-style-type: none"> If there are significant differences in costs (or benefits) between MS, what is causing them? How do these differences link to the intervention? What factors influenced the efficient functioning of the intervention and to what extent? What factors hindered it and to what extent? What is the connection between these factors and the actions laid out in Article 14? Which factors influenced the cost side and which ones influenced the benefit side? To what extent? To what extent were these factors linked to the intervention described in Art. 14? To what extent were there external factors that influenced the results? 	<ul style="list-style-type: none"> MD of eHealth Network members MS cost of implementation of developed tools DG REFORM capacity building budget Estimated benefits for the EU, Member States, Patients, HCP, Researchers, Industry. 	<ul style="list-style-type: none"> Accounting of MD spent (currently not monitored) Accounting of funds invested by MS in implementing the tools developed (currently not monitored) DG REFORM funds invested on capacity building Estimation of benefits: https://ehealth-impact.eu/
		<ul style="list-style-type: none"> Regulations linked to eHealth Network activities 	<ul style="list-style-type: none"> EUR-Lex MWP
		<ul style="list-style-type: none"> Internal and external factors affecting the efficiency of the developed tools and guidelines 	<ul style="list-style-type: none"> Focus Group Interviews
Relevance (A19)	<ul style="list-style-type: none"> To what extent are the objectives and provisions of Article 14 still relevant, considering current needs and how they have evolved since the adoption of the Directive? How relevant is article 14 to EU citizens? How did the article contribute to supporting citizens to access their own health data and ensure portability of these data? 	<ul style="list-style-type: none"> Revision of intervention logic needs and objectives 	<ul style="list-style-type: none"> The intervention logic developed in this report should be used as a baseline
	<ul style="list-style-type: none"> To what extent the provision of article 14 are relevant for the secondary use of health data (for policy making, regulatory purposes, research and innovation)? 	<ul style="list-style-type: none"> Mapping of rules to provide digital access to a copy of the medical record/s for patients affiliated to a healthcare system seeking cross-border healthcare in another Member State Mapping of rules to provide digital access to a copy of the medical record/s of received treatment/s for patients affiliated to a different healthcare system that used cross-border healthcare in another Member State 	<ul style="list-style-type: none"> Tables developed for this report should be used as a baseline (based on countries self-declaration in survey)
	<ul style="list-style-type: none"> To what extent have the original objectives proven to be appropriate to facilitate the cooperation and exchange of information between MS? 	<ul style="list-style-type: none"> Analysis of the needs relevant for the secondary use of health data and the objectives of Article 14 Level of achieved objectives and observed impacts 	<ul style="list-style-type: none"> Desk research Interviews Focus Groups The results of this study should be used as a baseline

Criteria	Research questions (RQ)	Indicators	Source
	<ul style="list-style-type: none"> How well adapted is Article 14 to subsequent technological or scientific advances (e.g. the use of Big Data and Artificial Intelligence in the field of healthcare)? To what extent does Article 14 facilitate both the processing of health data for treatment (e.g. through the eHealth Digital Service Infrastructure and the National Contact Points for eHealth), and further compatible processing of health data for research and policy-making? 	<ul style="list-style-type: none"> Analysis of the needs evolution linked to technological change and the objectives of Article 14 Analysis of MWPs and subsequent activities carried out 	<ul style="list-style-type: none"> Desk research Interviews Focus Groups <ul style="list-style-type: none"> Desk research Interviews Focus Groups
Coherence (A20)	<ul style="list-style-type: none"> To what extent are the provisions of Article 14 coherent with wider EU policy and with the European Health Data Space (especially the use of data for medical diagnosis, public health (including planning, provision of healthcare, management of health or social care systems and services, regulatory purposes, approval of medical devices, protecting against cross-border health threats) and for scientific or historical research and innovation)? To what extent is the cooperation described in art. 14 coherent with other Networks/cooperation possibilities which have similar objectives (especially for the use of data for policy making, research and innovation – eg Findata, French Data Hub etc)? To what extent is Article 14 coherent with international obligations? To what extent is the eHealth Network coherent internally (e.g. there is coherence between its actions/activities/tasks)? To what extent is the eHealth Network able to implement the European Health Data Space in its entirety, as requested by the mission letter of Commissioner Kyriakides? To what extent can Article 14 and the eHealth Network ensure that citizens have control over their own personal health data? 	<ul style="list-style-type: none"> Documentation and overview of other EU policies have been collected Objectives Activities and outputs carried out Amount of activities on cooperation with other networks Amount of activities on international cooperation Analysis of MWP Analysis of Output with respects to the European Health Data Space objectives Discussion on policy evolution (GDPR) and on Article 4.2 (f) and Article 5 (d) of the directive. 	<ul style="list-style-type: none"> Additional stakeholder/expert inputs on coherence with other EU policies should be collected eHealth Network cooperation with other networks eHealth Network deliverables on international cooperation MWP This report can be used as a benchmark Focus Groups
EU added value (A21)	<ul style="list-style-type: none"> What is the added value produced by the provisions of Article 14, compared to what could reasonably have been expected from the MS acting in the absence of the network at national or regional level? What would be the most likely consequences of stopping the eHealth Network/ repealing Art. 14? 	<ul style="list-style-type: none"> If common identification and authentication measures and platform running cross-border services would have been developed without eHealth Network. If yes, it would have been more or less effective. If common identification and authentication measures and platform running cross-border services would have been developed without eHealth Network. If yes, it would have been more or less effective. 	<ul style="list-style-type: none"> Study Survey Study Survey

Criteria	Research questions (RQ)	Indicators	Source
	<ul style="list-style-type: none"> How should the eHealth Network and article 14 be modified to increase their impact, especially in the light of new technological developments and the use of data, including for scientific research, policy making, reporting, protecting against cross-border health threats etc.? 	<ul style="list-style-type: none"> Discussion on new technological trends, cybersecurity and secondary use of data 	<ul style="list-style-type: none"> Focus Groups
	<ul style="list-style-type: none"> How should the tasks of the eHealth Network and article 14 be modified to increase their impact, especially in relation to setting up the European Health Data Space, ensuring the control of citizens over their own personal health data and the use of data for medical diagnosis, public health (including planning, provision of healthcare, management of health or social care systems and services, regulatory purposes, approval of medical devices, protecting against cross-border health threats) and for scientific or historical research and innovation)? 	<ul style="list-style-type: none"> Discussion on policy evolution and on Article 4.2 (f) and Article 5 (d) of the directive. 	<ul style="list-style-type: none"> Focus Groups
	<ul style="list-style-type: none"> What kind of cooperation at EU level would be most adequate for ensuring an adequate coordination of national efforts in the context of the European Health Data Space (especially to ensure access of citizens to their own health data, but also access to data for healthcare, research and policy making)? 	<ul style="list-style-type: none"> Discussion on policy evolution and on Article 4.2 (f) and Article 5 (d) of the directive. 	<ul style="list-style-type: none"> Focus Groups

8.6.2 Potential future financial inputs

Looking ahead at the EU's next multi-annual financial framework (MFF) for the period 2021-2027²⁴⁸, a number of funding instruments which could support targeted investment in the area of eHealth have been investigated. Financial instruments proposed under the next MFF may be divided into two main categories:

- **Shared management funds:** instruments whose management is shared between the EU and the Member States. In practice, Member States assume a large part of the responsibility for managing and distributing these funds via national implementing programmes, which are agreed and supervised by the Commission. The bulk of EU funds fall under this category.
- **Direct/indirect management funds:** instruments which are managed centrally and directly/indirectly by the European Commission, e.g. for research.

Following an assessment, a list of the financial instruments and programmes proposed that could be relevant for eHealth were mapped. These instruments and programmes could support targeted investment in the area of eHealth

Table 69. Next MFF instruments

Financial instrument or programme	Relevant sub instrument / programme	Investments/activities foreseen under the financial instrument or programme	Proposed amount in EURO
Shared management funds relevant for eHealth under the new MFF are managed by the Member States, through their managing authorities → also linked with the European Semester Process through the Country-Specific Recommendations	European Regional Development Fund (ERDF) ²⁴⁹	Investments in infrastructure; investment in access to services; productive investments in SMEs; equipment, software and intangible assets; information, communication, studies, networking, cooperation, exchange of experience and activities involving clusters; technical assistance	200.6 billion
	European Social Fund Plus (ESF+) ²⁵⁰	Strand for the European Social Fund Plus Strand for Health: analytical activities; policy implementation; capacity building; communication and dissemination activities	100 billion 413 million
	Recovery and Resilience Facility ²⁵¹	Loans and grants available to support reforms and investments undertaken by Member States. Each national recovery and resilience plan will have to include a minimum of 20% of expenditure to foster the digital transition.	134.5 billion (estimated from 20% of total)
Direct/indirect management funds relevant for eHealth under the new MFF	EU4Health ²⁵²	EU response to COVID 19 crisis. Among other things, digitalise healthcare through the creation and application of the European eHealth Record	9.4 billion
	The Digital Europe	High performance computing	2.7 billion
		Artificial Intelligence	2.5 billion
		Cybersecurity and trust	2.0 billion
		Advanced digital skills	700 million

²⁴⁸ The multiannual financial framework (MFF) is the EU's long-term budget. It sets the limits for EU spending - as a whole and also for different areas of activity - over a period of at least five years. Recent MFFs usually covered seven years.

²⁴⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A372%3AFIN>

²⁵⁰ https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-european-social-fund-plus-regulation_en.pdf

²⁵¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1602841299376&uri=CELEX:52020PC0408>

²⁵² https://ec.europa.eu/info/sites/info/files/about_the_european_commission/eu_budget/1_en_act_part1_v9.pdf

Financial instrument or programme	Relevant sub instrument / programme	Investments/activities foreseen under the financial instrument or programme	Proposed amount in EURO
	Programme (DEP) ²⁵³	Deployment, best use of digital capacity and interoperability	1.3 billion
	Connecting Europe Facility (CEF) ²⁵⁴	Digital connectivity infrastructure	3.0 billion
	The Invest EU Programme (InvestEU) ²⁵⁵	Sustainable infrastructure	11.50 billion
		Small businesses	11.25 billion
		Research, innovation & digitisation	11.25 billion
		Social investment & skills	4.0 billion
	The Reform Support Programme ²⁵⁶	Financial and technical support to implement reforms	25.0 billion
	The Horizon Europe Programme (HE) ²⁵⁷	Open Science	25.8 billion
		Global Challenges and Industrial Competitiveness	52.7 billion
		Open Innovation	13.5 billion

Source: Author's own evaluation

²⁵³ https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4043

²⁵⁴ <https://ec.europa.eu/inea/en/news-events/newsroom/commission-proposes-to-increase-connecting-europe-facility-funding>

²⁵⁵ https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_2135

²⁵⁶ https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3972

²⁵⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1540387631519&uri=CELEX%3A52018PC0435>

8.6.3 Multiannual Work Plan activities and outputs

Table 70. Mapping MWP 2012-2014 (eHGI JA)

Objectives	Activities	Outputs
Adopt common measures on eIdentification and authentication for eHealth under Directive 2011/24/EU, art.14	Policy paper "Conclusions on eID EU Governance for eHealth Services" - May 2012 eID & Authentication practices for eHealth in the EU Member States based on a questionnaire - November 2012 Position paper on the Commission proposal for an eID Regulation - May 2013 Road map giving a strategic approach to common measures on eID for eHealth under Directive 2012/24/EU and analysis of its implications (Risks, legal challenges, cost, benefits) - November 2013 Development of Common identification and authentication measures based on national solutions to support electronic transferring of data in cross-border healthcare settings.	Common identification and authentication measures based on national solutions to support electronic transferring of data in cross-border healthcare settings.
Addressing semantic and technical barriers to interoperability	Discussion paper on semantic and technical interoperability - November 2012 Semantic and technical interoperability roadmap (stepwise approach and intermediary milestones) - May 2013 development of Guidelines on semantic and technical interoperability	Guidelines on semantic and technical interoperability
Addressing legal barriers to interoperability, including data protection issues	Network's report on the Commission proposal for a Regulation on data protection November 2012 Legal Interoperability Roadmap for cross border exchange of electronic Health Records and ePrescriptions -2014	Guidelines on legal interoperability
Guidelines on patients' summary set of data for cross border electronic exchange, under the Cross border Directive	Non-exhaustive data set for patients' summary that can be exchanged across borders - November 2013 Guidelines on technical and semantic interoperability of the selected data set, including the coding, classification and terminologies set and their semantic transformation process in a multilingual environment - 2014	Guidelines on non-exhaustive list of data to be included in patient's summary Guidelines for cross-border electronic exchange of patients' summary data set
Guidelines on interoperability of ePrescriptions (art 11 of the Cross border Directive)	Discussion of the Network on interoperability of European and national databases for medicinal products - November 2012 Roadmap on interoperability of electronic prescriptions - 2013 Discussion paper on guidelines for electronic prescriptions - May 2014	Guidelines on interoperability of ePrescriptions
Sustainability	Development of recommendations on the governance of the Connecting Europe Facility (CEF) – May 2013	Recommendations on the governance of the Connecting Europe Facility (CEF)

Table 71. Mapping MWP 2015-2018 (JAsenHn)

Objectives	Activities	Outputs
Interoperability and standardisation;	Trusted eHealth National Contact Points. Propose an organizational framework to prepare, establish and govern eHealth National Contact Points in the scope of cross border care services deployed under the Connecting Europe facilities work plan.	Organisational Framework for National Contact Points for eHealth and several specific policy papers serving as the main basis for the preparation, deployment and operation of the National Contact Point for eHealth
	Electronic Identification for eHealth. Activities include the elaboration of an eID specific framework for eHealth representing an agreement primarily under the scope of the eID Regulation. This shall also include a set of common identification, authentication and authorisation measures based on national solutions to allow trusted electronic transfer of patient data in cross-border care. Further activities refer to the elaboration of guidelines on the interoperability of electronic professional registries and reports on notification of national eID under the scope of the eID Regulation.	<ul style="list-style-type: none"> (Legal) Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in CrossBorder eHealth Information Services
	Update & revision of EU eHealth Guidelines: Update and revise guidelines for Patient Summary, ePrescription and Patient Registries, which have been developed following former projects and been adopted by the eHN (except the Patient Registries guideline). The updating and revising process is necessary to ensure that requirements from the Member States and other stakeholders (incl. the input gathered by WP6) are taken into account for the development of further revisions. The aim is to maintain and provide a set of guidelines to foster semantic interoperability for cross-border exchange and to inform about the Member States' plans for national implementations.	<ul style="list-style-type: none"> Organisational Framework for National Contact Points for eHealth and several specific policy papers serving as the main basis for the preparation, deployment and operation of the National Contact Point for eHealth
	Alignment of standardisation	<ul style="list-style-type: none"> Refined eHealth European Interoperability Framework (ReEIF)
Exchange of Knowledge;	Analysis of the implementation of eHealth guidelines: The implementation analysis reflect various conditions in the Member States concerning the eHealth infrastructure in terms of legal, organizational and technical prerequisites for full guidelines adoption.	<ul style="list-style-type: none"> (Legal) Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services
	Development of legal interoperability in a cross-border context: This task concentrates on the creation of a sustainable legal basis for cross-border exchange of personal health data.	<ul style="list-style-type: none"> Refined eHealth European Interoperability Framework (ReEIF)
Assessment of implementation;	Sharing of National eHealth Strategies and Action plans	9 Documents on assessment of Member States policies and guidelines implementation
	Secondary use of Health Data: This task focused on: <ul style="list-style-type: none"> The pros and cons of the use of cloud computing in health, Publication of a code of conduct on how to handle secondary use of health data. Recommendation on de-identification of data for secondary use. 	
	Research on added value of eHealth Tools: This task explored and reported on the most up-to-date studies on the added value of eHealth services to health services	
	Participation, Liaison and Influence in global eHealth: This task is divided into the following sub-tasks: <ul style="list-style-type: none"> Overview of OECD studies on eHealth and core outcome 	

Objectives	Activities	Outputs
Global cooperation and positioning.	<ul style="list-style-type: none"> • Prepare for preparatory convergence meetings to coordinate input before WHO and OECD meetings on eHealth • <u>Information paper on main eHealth activities outside of the EU</u> <p>Evaluation of global eHealth specifications</p>	6 Documents on main eHealth activities outside of the EU and global eHealth specifications

Table 72. Mapping MWP 2018-2021 (EHAction)

Objectives	Activities	Outputs
Empowering people: enabling citizens to take an active role in the management of their health;	<p>mHealth and health apps reliability.</p> <ul style="list-style-type: none"> • Perform desk research including input from a consultation round with external stakeholders and input from JAseHN, and other projects. In addition, investigate ways to motivate or create incentives for patients to participate in their healthcare process by adopting and using mHealth services. • Analyse the findings and define a common understanding on the subject. • Develop a state of play/positioning report (common framework for the assessment/endorsement of health apps) with regard to mHealth and health apps reliability in relation to Patient Empowerment. • Participation to workshops to implement the MWP and coordinate dissemination activities. 	Develop a common framework and principles for facilitating safe and reliable use mHealth apps.
	<p>Patient access and use of data.</p> <ul style="list-style-type: none"> • Perform desk research; input from the consultation round with external stakeholders, JAseHN and other projects. In addition, investigate ways to motivate or create incentives for patients to participate in their healthcare process by accessing and using their health data. • Analyse the findings and define common understanding on the subject • Develop a state of play/positioning report with regard to patient access and use of data in relation to Patient Empowerment. • Participation to workshops to implement the MWP and coordinate dissemination activities. 	Synergetic and coherent approach to patient access, sharing, and reuse of health data in the EU.
	<p>Digital health literacy of patients.</p> <ul style="list-style-type: none"> • Starting with desk research including input from the consultation round with external stakeholders and input from JAseHN and other projects. In addition, investigate ways to motivate or create incentives for patients to participate in their healthcare process by increasing their digital health literacy. • Analyse the findings and define common understanding on the subject • Consult existing coalitions, such as https://ec.europa.eu/digital-single-market/en/national-local-coalitions • Develop a state of play/positioning report with regard to digital health literacy in relation to patient empowerment. • Participation to workshops to implement the MWP and coordinate dissemination activities. 	Increase digital health literacy for EU-citizens by sharing best practices and tools
	<p>TeleHealth.</p> <ul style="list-style-type: none"> • Perform desk research including input from the consultation round with external stakeholders. 	Facilitate the adoption of telehealth taking available evidence into consideration.
Innovative use of health data: exploring the use of health data to develop knowledge for healthcare policy and other purposes;	<p>Mapping, awareness raising and policy relevant actions on innovative use of big data in health.</p> <ul style="list-style-type: none"> • Compile policy relevant documentation including the EU Study and the effects of GDPR and review Member States/C policy level efforts on governing big data in health. • Also assess the implications of FAIR data principle. • Identify obstacles preventing Member States/C policies from being replicable either in another Member States/C or on EU level and investigate how to overcome these. • Provide an initial set of enabling actions for the information of the eHN by translating recommendations of the EU Study into operationalized solutions that can be communicated for increased awareness. 	Increase awareness on the possible impacts, challenges, risks and directions of Big Data in healthcare.

Objectives	Activities	Outputs
	<p>Sharing and learning best practices on European level.</p> <ul style="list-style-type: none"> Define and use methods to identify underlying needs and barriers experienced by stakeholders (pros & cons) affecting efficient and effective sharing of best practices in order to reach the objectives of the WP and the JA. Investigate already formalized cross-border use cases such as European Reference Networks for rare diseases as well as practical solutions in R&D including analytics in order to identify new possibilities for innovative use of big data on the European scale, to assess feasibility of network optimization to cross-border IT infrastructure and data flow management and to enhance interdisciplinary and openness, the most potential usage and stakeholders that could benefit. <p>Towards an attempt to define common principles for practical governance.</p> <ul style="list-style-type: none"> Make available guidance on practical governance for eHN and Member States. Provide a framework for the implementation of common principles for practical governance of big data including privacy protection and security aiming at improving health data transferability across borders with a special focus on data to be used in public health, research and quality assurance in healthcare on a European scale. The guidance will include guidance on implementation of data access and focus on helping Member States to utilize the potential of harnessing new opportunities arising from big data and improved data analytics capabilities, as well as from personalized medicine, use of clinical decision support systems by health professionals and use of mobile health tools for individuals to manage their own health and chronic conditions, in order to: <ul style="list-style-type: none"> facilitate preparation of actions to improve the comparability, accuracy and reliability of health data and to encourage the use of health data to enable more transparent and patient-centred health systems focusing on health outcomes and evidence-based health policy and decision-making, as well as to promote data-driven innovation; to enable the use of health data for research and innovation, in full compliance with data protection requirements and FAIR data principle; apply network optimization to cross-border IT infrastructure and data flow management; foster patient-centred interoperability; improve service effectiveness for the individual patient in which benefits are experienced locally; enhance interdisciplinary and openness that removes barriers between data sources and infrastructure to provide 'fit for purpose' data platforms. 	Common vision and priorities for innovative use of data in healthcare.
Enhancing continuity of care: improving the uptake of cross-border eHealth services;	Support of MyHealth@EU uptake. Support countries through eHMSEG for long term policy development in MyHealth@EU by facilitating the uptake of current use cases PS and eP/eD and especially the new ERN use case and by shaping an overall roadmap for MyHealth@EU use cases and additional features for a sustainable and continued usage of the NCPeH.	Full exploitation of the CBeHIS services.
	Support of legal MyHealth@EU matters. Support countries through eHMSEG by facilitating the national implementation of the MyHealth@EU legal environment (including but not limited to the eIDAS regulation, GDPR regulation, NIS directive and the Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services) by providing a forum for sharing expertise, problems and solutions and by synthesising shared elements into an MyHealth@EU legal report for a non-lawyer audience.	Identifying and developing new use cases and the sustainability of MyHealth@EU.
	eSkills for Professionals. Support countries through eHMSEG by developing a process to ensure that the eSkills necessary to gain full advantage from the implementation of European eHealth Strategies and cross-border healthcare services, identifying current challenges and appropriate actions that can be taken to build the necessary eSkills framework for healthcare professionals.	Equip healthcare professionals with eSkills for eHealth services.

Objectives	Activities	Outputs
<p>Overcoming implementation challenges: addressing transversal enabler issues crossing the abovementioned categories.</p>	<p>Recommendations on how to implement interoperability guidelines in large health-care organisations. Interoperability has long been identified as the fundamental facilitator of communication, exchange and use of patient information between healthcare providers, hospitals, government, insurers etc., especially in the context of cross-border health services. During the past decades various standards have been developed regarding messaging (HL7, DICOM, ASC-X12, IEEE 1073 etc.), terminology (ICD-10, ICD-11 which is due by 2018, LOINC, SNOMED CT etc.), documents, conceptual frameworks, application and architectures, both for syntactic interoperability, and for semantic interoperability. Nevertheless, and despite the efforts, interoperability is still considered as an "open field" in the healthcare ecosystem, especially when striving to provide cross-border health services.</p> <p>The aim of this task is to exploit any previous work in the field of interoperability as described in the Digital Agenda, the eHealth Action Plan, the "Refined European eHealth Interoperability Framework" (reEIF), the epSOS project, SemanticHealthNet, JAseHN and more, in order to facilitate patients' rights in cross-border healthcare. All previous work will be combined to produce recommendations for IT Management on how to implement interoperability guidelines in large healthcare organizations (e.g. hospitals). The main purpose is to align all work done about various EU regulations/common frameworks and provide it to IT Management of hospitals for implementation. The deliverables of this task will provide recommendations, guidelines to facilitate implementation of the interoperability framework by hospital IT management staff taking into consideration the recommendations included in the new European Interoperability Framework (EIF). Hospital experts will contribute to this task with F2F Workshops. The task will be implemented in the following steps:</p> <ul style="list-style-type: none"> • Review of previous work, interoperability frameworks and standards that can be implemented from the IT departments in healthcare organizations • IT challenges in implementing interoperability in/ between large healthcare organizations • Recommendations, guidelines and priorities for IT Management on implementing interoperability actions in healthcare organizations. • Interoperability guidelines for hospital IT management staff in the following cases: <ul style="list-style-type: none"> ◦ Software supply ◦ Software building ◦ Software deployment 	<p>Interoperable digital infrastructure (software and hardware) of healthcare providers using a common format for cross-border exchange of health data.</p>
	<p>Data protection.</p> <p>This task will focus on the GDPR implementation and its implications in cross border healthcare. The aim of this task will be to share best practices and approaches on data protection at national level. Situation regarding data protection and the new requirements GDPR brings in eHealth. It is proposed to implement the topic in 5 steps:</p> <ol style="list-style-type: none"> 1. Review of the GDPR topic in general and view of its impact on the healthcare stakeholders. 2. Characteristics of main points and requirements of GDPR adoption in the healthcare sector. 3. Proposal of the set of relevant recommendations/policies for successful completion of GDPR adoption in the healthcare sector. 4. Sketches of collaborative instruments for related information and education in current and future dealing with GDPR topic in the healthcare settings. 5. Foresight – vision and mission - of the future fulfilment and development of the GDPR. <p>The task is motivated by both urgent needs for correct GDPR adoption in the healthcare sector and the utilization of GDPR potential for comprehensive respecting human rights for the healthcare provision practice in long-term run.</p>	<p>Increase trust in eHealth by overcoming the implementation challenges of the relevant EU legal frameworks on data protection, security, authentication of the actors, and privacy.</p>

Objectives	Activities	Outputs
	<p>In topics No. 2, 3 and 5 the cooperation with public interest groups (patient and healthcare professionals' organizations) will be actively sought and utilized.</p> <p>Data and systems security. The aim of this task is to create a common Framework for cyber security for eHealth systems</p>	

8.6.4 Future activities

In terms of future activities, on June 2019, the Common Semantic Strategy (CSS) group of the eHealth Network, developed a multiyear plan to set priority until 2025²⁵⁸.

Whereas the focus in 2021 will be on the capacity of the CSS Committee, capacity building beyond that year will have to address other international and especially national experts in order to be able to transfer the work and knowledge from the CSS to national groups and users. This will enable countries to fully consider benefits and inputs of recommendations and will hopefully foster the adoption of EU suggestions in Member States/C.

In 2022, Laboratory Reports will be addressed and the work on the Discharge Reports will continue.

In 2023, Image Reports will be addressed and work on Laboratory Reports will continue. Discharge Reports will be finalised, and a recommendation is expected to be available at the end of the year.

In 2024, Laboratory Reports will be finalised, and a recommendation is expected; work on Image Reports will continue; and evaluation documentation on the rationale, working method and effectiveness of the group will be started.

In 2025, recommendations on Discharge, Laboratory and Image Reports will be available, as well as an evaluation of the rationale, working method and effectiveness of the group. The evaluation documentation will be provided early in the Year 5, in order to decide on the continuity of the group after the initial five years. Together with the evaluation documentation, a plan for next steps in the Common Semantic Strategy will be provided. The goals, objectives and activities of this plan are summarised in the table below.

²⁵⁸ https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co242_en.pdf

Table 73. Common Semantic Strategy (CSS)

Goal	Description	Objective	Activity
G1	Structuring a common approach on health semantics in the EU	O1.1 Realise a Common Semantic Strategy for Health in the EU	A1.1.1 Propose a 5-year CSS to the eHN A1.1.2 Analyse data availability, standards in use and information exchange flows in MS/C. A1.1.3 Structure a learning programme to assist capacity building in MS/C
		O1.2 Develop common semantic artefacts for PS, eP, lab requests and results, medical imaging and reports, hospital discharge reports	A1.2.1 Publish common semantic artefacts for the chosen semantic domains A1.2.2 Setup common semantic resources: "Common European Healthcare Semantic Server"
		O1.3 Provide guidelines for the standards adoption	A1.3.1 Study the data availability and standards in use in the different MS/C A1.3.2 Define a set of common standards for the cross-border exchange of health information
		O1.4 Establish a solid relationship with key bodies of the EU and key technological partners	A1.4.1 Liaison with key partners such as SDOs, technology developers etc. relevant to the CSS A1.4.2 Establish a routine exchange format with key bodies of the EU relevant to the CSS
G2	Providing guidance for EU level decisions on health semantics	O2.1 Establish mechanism/ methodology to audit conformance issues at an EU level.	A2.1.1 Propose a mechanism to build capacity in MS/C to foster the use of EU semantic standards for cross-border healthcare
		O2.2 Establish a mechanism to participate in the approval of EU semantic artefacts and projects	A2.2.1 Propose a mechanism to participate in the approval of EU semantic artefacts and projects to the eHN
G3	Ensuring stability and continuity on health semantics in the EU	O3.1 Establish a CSS Committee	A3.1.1 Get a mandate from the eHN
			A3.1.2 Get representatives from each MS/C to join the Committee

Source: eHealth Network

8.6.5 Examples of European funded projects in eHealth

Acronym	Project title
PHIRI	Population Health Information Research Infrastructure
InfAct	Information for Action
ImpleMentAll	Towards evidence-based tailored implementation strategies for eHealth
CONNECARE	Personalised Connected Care for Complex Chronic Patients
BRIDGE-Health	BRIdging Information and Data Generation for Evidence-based Health Policy and Research
EUCANCan	EUCANCan: a federated network of aligned and interoperable infrastructures for the homogeneous analysis, management and sharing of genomic oncology data for Personalized Medicine.
CINECA	Common Infrastructure for National Cohorts in Europe, Canada, and Africa
euCanShare	An EU-Canada joint infrastructure for next-generation multi-Study Heart research
RECODID	Integrated human data repositories for infectious disease-related international cohorts to foster personalized medicine approaches to infectious disease research
EUCAN-Connect	A federated FAIR platform enabling large-scale analysis of high-value cohort data connecting Europe and Canada in personalized health
EOSC-Life	Providing an open collaborative space for digital biology in Europe
MultipleMS	Multiple manifestations of genetic and non-genetic factors in Multiple Sclerosis disentangled with a multi-omics approach to accelerate personalised medicine
PanCareSurPass	PanCare studies of the scale-up and implementation of the digital Survivorship Passport to improve people-centred care for childhood cancer survivors
U-PGx	Ubiquitous Pharmacogenomics (U-PGx): Making actionable pharmacogenomic data and effective treatment optimization accessible to every European citizen
EJP RD	European Joint Programme on Rare Diseases
ImmunAID	Immunome project consortium for AutoInflammatory Disorders
Solve-RD	Solving the unsolved Rare Diseases
ORCHESTRA	Connecting European Cohorts to Increase Common and Effective Response to SARS-CoV-2 Pandemic: ORCHESTRA
EXSCALEATE4CoV	EXaSCale smArt pLatform Against paThogEns for Corona Virus
CORESMA	COVID-19-Outbreak Response combining E-health, Serolomics, Modelling, Artificial Intelligence and Implementation Research
EpiPose	Epidemic intelligence to minimize 2019-nCoV's public health, economic and social impact in Europe
TIMESPAN	Management of chronic cardiometabolic disease and treatment discontinuity in adult ADHD patients
REALMENT	Using real-world big data from eHealth, biobanks and national registries, integrated with clinical trial data to improve outcome of severe mental disorders
RETENTION	heaRt failurE paTient managEment and iNTerventiOns usiNg continuous patient monitoring outside hospitals and real world data
R-LiNK	Optimizing response to Li treatment through personalized evaluation of individuals with bipolar I disorder: the R-LiNK initiative
SYNCHROS	SYNergies for Cohorts in Health: integrating the ROle of all Stakeholders
HarmonicSS	HARMONIzation and integrative analysis of regional, national and international Cohorts on primary Sjögren's Syndrome (pSS) towards improved stratification, treatment and health policy making
HealthyCloud	HealthyCloud – Health Research & Innovation Cloud
PROTECT	Pharmacoepidemiological research on outcomes of therapeutics by a European consortium

Acronym	Project title
U-BIOPRED	Unbiased biomarkers for the prediction of respiratory disease outcomes
EHR4CR	Electronic Health Records Systems for Clinical Research
EMIF	European Medical Information Framework
eTRIKS	Delivering European Translational Information & Knowledge Management Services
GetReal	We facilitate the adoption and implementation of RWE in health care decision-making in Europe
ROADMAP	Real world Outcomes across the AD spectrum for better care: Multi-modal data Access Platform
DO->IT	Big data for better outcomes, policy innovation and healthcare system transformation
BigData@Heart	Big data at heart
C4C-Paediatric network	COllaborative Network for European Clinical Trials For Children
European Health Data Network (EHDN)	Health data
MIDAS	Big Data, Open Data, Heterogeneous Health Care Data, My Data, Health in all Policies
PD manager	mhealth platform for Parkinson's disease management
myAirCoach	Analysis, modelling and sensing of both physiological and environmental factors for the customized and predictive self-management of Asthma
GenoMed4ALL	Genomics and Personalized Medicine for all though Artificial Intelligence in Haematological Diseases



Publications Office
of the European Union

ISBN 978-92-76-47023-6